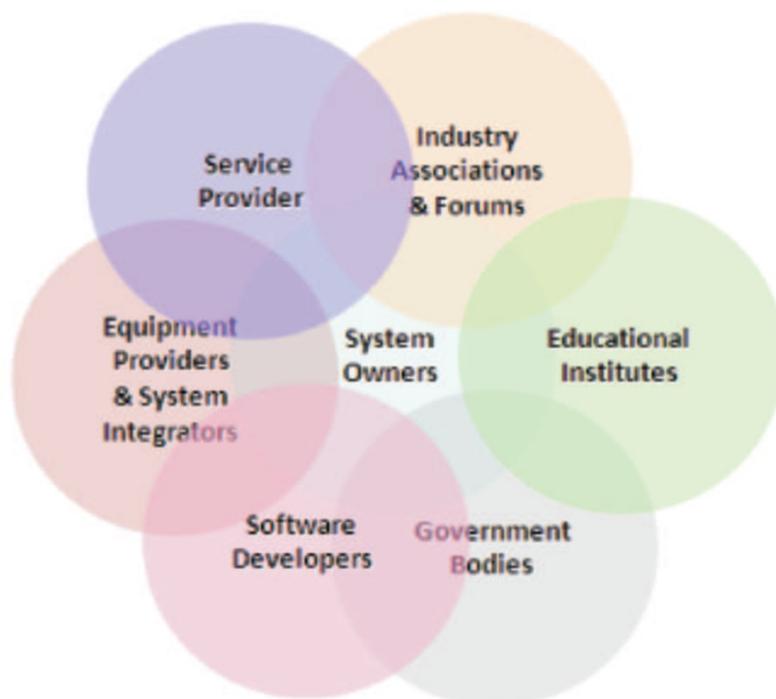




सत्यमेव जयते

National IPv6 Deployment Roadmap



Government Of India
Ministry of Communications and Information Technology
Department of Telecommunications

National IPv6 Deployment Roadmap ver 1.0

First Published: June 2010

Telecommunication Engineering Centre
Department of Telecommunications
Government of India
Khurshid Lal Bhawan, Janpath
New Delhi – 110001
India

Disclaimer

This document is meant for circulation amongst the stakeholders in the telecom field and for information of students. The information contained is mostly compiled from different sources and no claim is made for being original. Every care has been taken by the authors to provide most up-to-date and correct information along with the references thereof. However, neither TEC nor the authors shall be liable for any loss or damage whatsoever, including incidental or consequential loss or damage, arising out of, or in connection with any use of or reliance on the information in this document. In case of any doubt or query, readers are requested to refer to the detailed relevant documents.

Dated: 11th June, 2010

FOREWORD

Telecommunications has vast impacts on the infrastructure and economy of our country and touches every person's life in many ways through Information and Communication Technologies. With the passage of time, we are seeing major technology changes leading to dominance of packet switched networks. The Internet Protocol, which runs all packet based networks, is evolving as a global standard for communication across the world. The current deployment of IP networks uses IPv4 addresses. IPv4 has now been left with limited addresses. While IPv6, with practically unlimited addresses, is having many more features over IPv4 capability. Therefore, for the continued growth of the Internet and the numerous possibilities of new kinds of networks and services in future, it is time that service providers and all other stakeholders take an active interest to plan for a smooth transition to the next generation internet protocol IPv6.

TEC has taken up a number of activities to facilitate IPv6 deployment in the country. We have been conducting IPv6 workshops throughout the country to build awareness and momentum in this area. After consultations with all stakeholders, TEC has prepared this "National IPv6 Deployment Roadmap" and it is hoped that this document will prove to be an important milestone in shaping the IPv6 future of the country. I hope, with this initiative and the support of all stakeholders, we shall be able to make India IPv6 ready in a timebound manner.



(N.K. Srivastava)

Sr. Dy. Director General
Telecom Engineering Center

Document History Sheet

Sr.No.	Version / Revision	Date	Description	Prepared by
1.	V 1.0	June,2010	First Version	R.M.Agarwal, DDG(SA), TEC B.K.Nath, Dir(SA), TEC

Executive Summary

The Internet today has become a global network serving billions of users worldwide and this has happened because of the wide acceptability of the Internet protocol. The current version of the Internet Protocol is IPv4 which is a 25 year old protocol having many limitations. The biggest limitation is its 32-bit addressing space of about 4.3 billion IP addresses. The rapid growth of Internet, wireless subscribers and deployment of NGN technology is leading to accelerated consumption of IP addresses, and this will result in exhaustion of IPv4 addresses in coming years. It is expected that existing pool of IPv4 addresses will exhaust by August-2012. To overcome this problem of shortage, Internet Protocol version 6 (IPv6) was developed by the Internet Engineering Task Force(IETF), which improves on the addresses capacities of IPv4 by using 128 bits addressing instead of 32 bits, thereby practically making available an almost infinite pool of IP addresses. Also IPv6 is supposed to provide various enhancements with respect to security, routing addresses, auto configuration, mobility and Quality of Service (QoS) etc.

The various policies of the Government(s) to increase the penetration of Broadband and Internet will lead to surging demand for IP addresses. Therefore, worldwide, different countries are implementing the new IPv6 addresses to accommodate increased number of users and also develop applications based on the new features of the protocol. Therefore, different countries are making all out efforts to migrate from IPv4 to IPv6 on priority in order to remain globally competitive.

In India also, efforts began as early as 2004 when “Migration from IPv4 to IPv6 in India” was listed as one of the items in the Ten Point Agenda given by Hon’ble Minister of Communications & Information Technology, Government of India. After due deliberations a Committee under the Chairmanship of Advisor(T), DoT was formed in DoT and recommended for preparing a suitable Roadmap to achieve transition from IPv4 to IPv6, clearly bringing out the steps involved.

The task of leading the country towards IPv6 was given to Telecommunication Engineering Centre (TEC), a standardization body under the Department of Telecommunications (DoT) in 2009. Keeping all the issues in mind deliberations were initiated with industry members and service providers, and it is emerged from all these discussions that there is a need to crystallize and firm up the transition strategy from IPv4 to

IPv6 by involving all stakeholders. Since then TEC has conducted with CMAI a number of activities, like workshops, seminars, training programmes etc. throughout the country to interact with different stakeholders like service providers, central and state government departments, educational institutions, industry associations, equipment manufacturers, content developers etc. Based upon the inputs received from different stakeholders TEC has prepared the “**National IPv6 Deployment Roadmap**”, which examines the different issues related to the deployment of IPv6 in India.

Since the IPv4 addresses are expected to be exhausted by August-2012, it is expected that all service providers and other stakeholders will transit to IPv6 in a time-bound manner. On interaction with different service providers, it is found that some of them are in a good position whereas others, especially the smaller and medium service providers, will have to make more efforts to start offering IPv6 services before exhaustion of IPv4 addresses. In this document separate transition timeframes have been suggested for government departments and service providers and they shall adhere to these timeframes.

During the interactions with different stakeholders it was suggested to create a common platform for discussing and resolving issues related to IPv6 migration and potential. Accordingly in this document it has been recommended to create a multimember **IPv6 Task Force**, having representation from all the stakeholders. This Task Force will have different working groups, which will take up specific activities in different areas for IPv6 deployment in the country. Each working group will work under the leadership of one of the member organizations of the Task Force. On a long term basis, it has been suggested to create a national centre of excellence on IPv6 called “Indian IPv6 Centre for Innovation”, which will take over all the activities of the Task Force in addition to others in due course of time.

Adoption of IPv6 at the earliest will not only meet the requirement of IPv4 address shortage but will also provide the potential for innovative applications in different sectors. Few such applications have been dealt in this document as an indicative measure.

This document has been prepared to show the path for successful deployment of IPv6 in India in a time bound manner with the active involvement of all stakeholders.

ACKNOWLEDGMENTS

The Internet has come a long way over the last 25 years from being a university research project to serving numerous organizations across the globe. But the Internet we know today is widely based on IPv4. Modern communication demands far greater capabilities which IPv4 cannot provide because it was not designed that way. Therefore, time has come for transition to the next generation IPv6 protocol. Our country is also moving in this direction but needs a definite roadmap to achieve the transition in a timebound manner. During the last one year lot of interactions happened with different stakeholders during different IPv6 events and the suggestions, opinions and feedback given by everyone have culminated into this report. Many of the valuable inputs for this report were received during the various IPv6 workshops during 2009-10, which TEC/DoT had conducted throughout the country for interaction with stakeholders like service providers, industry associations, Educational Institutions, different government departments and ministries, Industry Forums etc.

We are thankful to Shri P.J.Thomas,Secretary(T); Shri Chandra Prakash, Member(T); Shri S.C.Misra, Member(Services); Smt. Vijayalakshmy K. Gupta, Member(Finance); Shri D.K.Agrawal, Advisor(T); Sh.Subodh Kumar, Addl.Secretary(T); Shri Ajay Bhattacharya, Administrator(USOF); Shri Kuldeep Goyal, CMD BSNL; Shri Kuldip Singh, CMD MTNL and Sh.N.Ravi Shanker, Jt. Secretary,DIT for their constant encouragement and support during the workshops and preparation of this roadmap.

We take this opportunity to express our thanks to Shri N.K.Srivastava, Sr.DDG TEC without whose guidance and support we could not have reached this stage. We are also thankful to various inputs and support given by DoT and TEC officers. Our special thanks to Shri Nitin Jain, DDG(DS), DoT and Shri Subodh Saxena, Dir(DS-II), DoT for providing us regular inputs and doing peer review of the report. We are also thankful to Shri N.K.Goyal, President CMAI and his dedicated team for conducting the IPv6 workshops in the country.

We are specially thankful to the representatives of Industry associations like COAI, CMAI, AUSPI, TEMA, ISPAI, IPTV Forum, ACTO, OSPAI and others for their active participation in different IPv6 related activities and making them successful.

We would also like to give special thanks to the IPv6 Forum members Shri Latif Ladid IPv6 Forum President; Mr. Hiroshi Esaki, Chairman, IPv6 Ready Logo; Mr. Hiroshi Miyata, Leader, TAHI Project Japan; Shri Jai Chandra, President, IPv6 Forum India; Shri Hemanth Dattatreya, Vice-President, IPv6 Forum India and others for their continuous involvement in the workshops and other IPv6 activities.

We are also thankful to the various speakers from TRAI, DIT, BSNL, MTNL, IISc Bangalore, IIT Chennai, IIT Mumbai, IIT Kanpur, ERNET, CISCO, TATA Communications, Spectranet, TTSL, Bharti Airtel, Inspira Enterprises, Hewlett Packard India, Railtel, Orange, Alcatel-Lucent, SIFY, Tech Mahindra, iRAM Technologies and many others who have attended the various IPv6 workshops and gave important suggestions and contributions for shaping the report. We are also thankful to speakers from M/s Infoweapons, Phillipines; Hurricane Electric USA, Asia Pacific Network Information Centre (APNIC), Internet Society Australia and 6Choice Europe who attended the International IPv6 summit in India and gave their global perspective on IPv6.

We would like to thank everyone once again for contributing directly or indirectly during the preparation of this report.

R.M.Agarwal, DDG(SA), TEC, New Delhi
B.K.Nath, Dir(SA), TEC, New Delhi

CONTENTS

		Page
1	IPv6: The Next Generation Internet (An Overview)	1-18
1.0	Introduction	2
1.1	IP, IPv4 and IPv6	2
1.2	Limitations of Existing Internet based on IPv4	3
1.3	State of IPv4 in the World	4
1.4	Extending Availability of IPv4 Addresses	5
1.5	IPv6: The best way forward	7
1.6	Advanced Features in IPv6	7
1.7	Interworking IPv4 and IPv6	10
1.8	Stakeholders in the Transition Process	12
1.9	Some IPv6 Initiatives around the World	13
1.10	Maintaining India's competitiveness and development in the country	17
1.11	Objective of this Document	18
2	IPv6 initiatives in India by Telecommunication Engineering Centre and DoT	19-31
2.0	Policy decisions taken by DoT	20
2.1	Telecommunication Engineering Centre (TEC)	21
2.2	Workshops Conducted by TEC	22
2.3	Summary of Outcome of the TEC Workshops and Other activities of the Government	30
3	Transition Plan for Government Departments	32-49
3.0	Introduction	33
3.1	Steps: Governments Departments/organizations can follow	33
3.2	Management Structure for IPv6 Deployment in Government Departments	34
3.3	Appointment of Nodal Officers	35
3.4	Functions of the Nodal Officer	35
3.5	Issues that need to be addressed by the departmental cross-functional team during transition	36
3.6	Issues that need to be addressed in the Departmental transition plan	36
3.7	Recommended Phase wise IPv6 Implementation by the Government Departments	36
3.8	Other important aspects to be considered by the organizations	43
3.9	Modified Approach due to Time Constraints	46
3.10	Recommended Approach for India	46
3.11	Time plan for migration	47
3.12	Actionable points	49

4	Action Plan for Service providers	50-62
4.0	Introduction	51
4.1	Discussions with Service Providers on Transition Plan	51
4.2	Time Plan for Transition	58
4.3	Action Plan for the ISPs	59
4.4	Action Plan of ASP/CSP	62
4.5	Actionable points	62
5	India IPv6 Task Force	63-78
5.0	Introduction	64
5.1	Duration of Existence of the Task Force	64
5.2	Action Items for the Task Force	65
5.3	Structure of Task Force	68
5.4	Member Organizations	71
5.5	Working Groups	72
5.6	Distribution of Working Groups between Different Service providers	75
5.7	Human Resource Requirements	76
5.8	Funding Model and Budget Requirements for the Task Force	76
5.9	Creation of “Indian IPv6 Centre for Innovation” as a Long term alternative to Task Force	77
5.10	Actionable Points	78
6	IPv6 Standards and Certifications	79-87
6.0	Introduction	80
6.1	Japanese initiatives in development of specifications	80
6.2	Several Successful efforts under the WIDE Project for IPv6	81
6.3	The TAHI Project	81
6.4	Certification of Products (IPv6 Ready Logo Program)	81
6.5	IPv6 Ready Logo Committee	82
6.6	Different Phases of the IPv6 Ready Logo Program	83
6.7	Writing Test Specifications	84
6.8	Certification of services (IPv6 Enabled Logo Certification for ISPs)	84
6.9	US Initiatives in the Development of Specifications (USGv6 / NIST IPv6 Testing)	84
6.10	Recommendations for India	85
6.11	Actionable Points	87
7	IPv6 Adoption: A New Way Ahead	88-97
7.0	Introduction	89
7.1	Logistics and Supply Chain in Indian Railways	91
7.2	Intelligent Transport System	92
7.3	Rural Emergency Health Care	93
7.4	Smartgrids for Power Distribution	96

8	Indian IPv6 Centre for Innovation	98-110
8.1	Introduction	99
8.2	Similar Initiatives in Other Countries	99
8.3	Development in India	101
8.4	Proposed Activities of the Indian IPv6 Centre for Innovation	102
8.5	Structure of the Indian IPv6 Centre for Innovation	104
8.6	Working Groups and their Functions	106
8.7	Initial Cost, Budget and Funding of the organization and the working groups	109
8.8	Human Resource Requirements	110
9	Action Items	111-115
10	References	116-117
11	Annexures	118-132
A	Checklist for Migration from IPv4 to IPv6 in India	118
B	Checklist for Assessment of Existing Network Infrastructure	121
C	IPv6 Migration Strategies	126
12	Glossary	133-136

LIST OF TABLES

Table No.	Description	Page No.
1	IPv4 Address Allocation to Different Countries	4
2	Action Plan for Government Departments	48
3	Action Plan for Network Players (ISPs)	60
4	Action Plan for Service Area (ASP / CSP)	61
5	Allocation of Working Groups to Service providers / Organizations	76
6	Advanced Features of IPv6	89
7	IPv6 Technologies – Enabling Next Generation Healthcare	94
8	Technologies for Healthcare	95

LIST OF FIGURES

Figure No.	Description	Page No.
1	IPv4 Address Scheme	3
2	IPv6 Address Scheme	3
3	IPv4 Address Exhaustion Timeframe	3
4	Comparing of IPv4 and IPv6 Headers	9
5	Dual Stack Mechanism	11
6	Tunelling Mechanism	11
7	Structure of IPv6 Group in Ministry / Department / PSU	35
8	Structure of India IPv6 Task Force	67
9	Composition of Oversight Committee	68
10	Composition of Steering Committee	69
11	Schematic of IPv6 Implementation in Railways	92
12	Schematic of Intelligent Transport System	93
13	An IPv6 Based Emergency Healthcare System	96
14	IPv6 Based Smartgrid Schematic	97

	1
--	----------

<p>IPV6: The Next Generation Internet (An Overview)</p>
--

1.0 Introduction

The Indian economy has received a significant boost during the last decade with huge growth in telecom subscriber base as well as Internet usage. India did well in investing in dark fiber infrastructure in the earlier part of this decade the benefits of which the country is reaping now. At the end of March 2010, India had 621.28 million subscribers out of which about 584.32 million was wireless ,next only to China, thus making India the second largest in the World.

However, telecommunication technology itself is undergoing dynamic change in the world and is moving towards the Internet and Internet technologies. The Internet today has become a global network serving billions of users worldwide. It has become popular because of its ability to extend **accessibility to Everyone, Anywhere and Anytime**. The vehicle of the Internet is the “Internet Protocol” which assigns any router, server, host or simple internet device such as mobile phone, Internet Phone or sensor and radio frequency identification device (RFID) an address so that it can communicate with other similar internet devices. The **Internet Protocol** is evolving as the **Global Standard** for communication across a range of devices, platforms and networks across the world.

1.1 IP, IPv4 and IPv6

The “Internet Protocol” (IP) is one specific element of the Internet architecture. Most parts of the Internet today run using **Internet Protocol Version 4 (IPv4)**¹ addresses. An IPv4 address has a 32-bit addressing space, which can theoretically cater to $2^{32} = 4.3$ billion devices. At the end of 2009, the world population is estimated to be 6,794,600,000². If every person on this planet is associated with at least one internet access device, it is evident that we don't have enough IPv4 addresses. This was foreseen in the early 1990s itself and therefore the **Internet Protocol Version 6 (IPv6)** was developed. Apart from increasing the address space to 128 bits, many new and advanced features were also introduced in IPv6,

¹ IPv4 is specified in RFC 791, 1981. RFC stands for “Request for Comments”

² http://en.wikipedia.org/wiki/World_population accessed on 06/01/2010

which are not present in IPv4. IPv6 has been designed ground up, therefore, IPv6 is not backward compatible with IPv4.

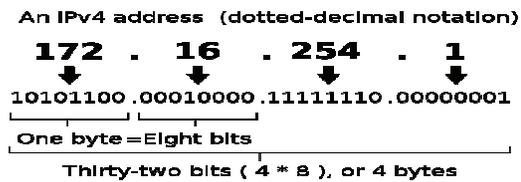


Figure 1: IPv4 Address Scheme



Figure 2: IPv6 Address Scheme

1.2 Limitations of Existing Internet based on IPv4

The current generation of the Internet runs mostly on the IPv4 protocol. It was a protocol designed by the Internet Community almost 27 years ago for use in academic environments. It was never really designed to work in the commercial world.

The most important limitation of IPv4 is that its has an address space of only 32 bits thereby limiting the total number of addresses to about 4 billion only to be used globally. The rapid growth of Internet and deployment of NGN technology is leading to accelerated consumption of IP addresses, and this will result in shortage of IP addresses in coming years. It is expected that existing pool of IPV4 addresses will exhaust by mid-2012.

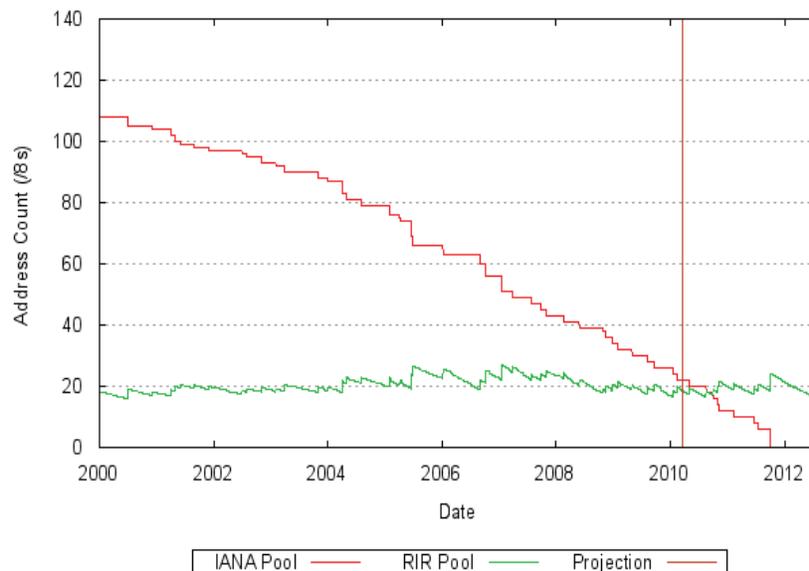


Figure 3: IPv4 Address Exhaustion Timeframe

To overcome this problem of shortage, Internet Protocol version 6 (IPV6) was developed by the Internet Engineering Task Force(IETF),which improves on the addresses capacities of IPV4 by using 128 bits addressing instead of 32 bits, thereby making available an almost infinite pool of IP addresses i.e. 2^{128} . Also IPV6 provides various enhancements with respect to security, routing addresses, auto configuration, mobility and QoS etc.

1.3 State of IPv4 in the World

In the beginning, during the 1980's, 4.3 billion IPv4 addresses was considered to be huge. Therefore, many organizations in those days, took far too many addresses than what they needed. By 1990 almost 50% of the addresses had been handed out. Later on International organizations like the ICANN and the Regional Internet Registries (like APNIC) evolved policies to control new assignments of IP addresses to demonstrated need. Presently the remaining IPv4 address space is down to just 6.25% (16/256 blocks) as of May 2010. Therefore, the IP address distribution among different countries of the World is much skewed. The address space has now become a scarce resource which will not be enough to sustain the continuing growth of the Internet. The position of different countries with respect to allocation of IPv4 addresses is given below.

Table 1: IPv4 Address Allocation to Different Countries

Country	Country Code	Addresses(million)	Addresses Per Capita
United States	US	1474.319	5.297
China	CN	194.425	0.152
Japan	JP	153.327	1.210
European Union	EU	114.103	-
Germany	DE	85.300	1.038
Canada	CA	76.197	2.446
South Korea	KR	72.239	1.542
United Kingdom	GB	70.795	1.187
France	FR	68.385	1.155
Australia	AU	37.378	1.979
Italy	IT	32.344	0.561
Brazil	BR	29.755	0.175

Russian Federation	RU	24.919	0.170
Taiwan	TW	24.681	1.109
Spain	ES	22.065	0.559
Mexico	MX	21.503	0.217
Netherlands	NL	21.249	1.339
Sweden	SE	18.998	2.144
India	IN	18.312	0.018

It is seen that as of 2009, India has 18.2 million IPv4 addresses, with less than 0.018 IP address per India citizen. One may wonder that if India has so little IPv4 addresses then how it is managing so many internet users, which is far greater than 18 million. This is because of the extensive use of Network Address Translation (NAT)³. The US has the largest chunk of IPv4 addresses extending 5.3 IP address per US citizen. China also has a large chunk of IPv4 addresses though it is still 0.15 addresses per capita. A limited number of new IPv4 addresses can be obtained until the APNIC pool dries out by 2012. How to deal with this transition is currently the subject of discussion in the Internet community in general, and within and amongst the RIR communities in particular. *All RIRs have recently issued public statements and have urged the adoption of IPv6.*

1.4 Extending Availability of IPv4 Addresses

- (i) **Network Address Translation (NAT)**⁴ - NATs connect a private (home or corporate) network which uses private addresses to the public Internet where a single public IP address is required. Private addresses are blocks of addresses reserved for that purpose. The NAT device acts as a gateway between the private network and the public Internet by translating the private addresses into a single public address. This method therefore reduces consumption of IPv4 addresses. However the usage of NATs has two main drawbacks, namely –
 - a. **It hinders direct end-device-to-end-device communication** - Intermediate NAT devices are required to allow hosts or devices with private addresses to

³ Network Address Translation – It is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping a given address space to another. The NAT device maintains translation tables to do this remapping.

⁴ RFC 2663, 1994

communicate across the public Internet. NAT effectively turns an Internet connection into a one-way channel (from user to content provider), making it very difficult for most users to accept incoming connections. This requires “NAT traversal” (e.g. STUN) which greatly complicates application design and implementation, and leads to serious security issues with most firewalls.

- b. **Adds Complexity**- It adds a layer of complexity in that there are effectively two distinct classes of computers - those with a public address and those with a private address. This often increases costs for the design and maintenance of networks as well as for the development of applications.

Apart from NAT mentioned above some other measures can also extend the availability of IPv4 addresses.

- (ii) A market to trade IPv4 addresses might emerge which would offer incentives to organisations to sell addresses they are not using. However IP addresses are not strictly property. They need to be globally acceptable to be globally routable which a seller cannot always guarantee. In addition they could become a highly priced resource. So far RIRs have been sceptical about the emergence of such a secondary market.
- (iii) Another option consists of trying to actively reclaim those already-allocated address blocks that are under-utilised. However, there is no apparent mechanism for enforcing the return of such addresses. The possible cost of it has to be balanced against the additional lifetime this would bring to the IANA pool. According to the 2008 OECD report on IPv6, any attempts to “recover” lost addresses would be very expensive, take years to accomplish, and each recovered “/8” would extend the lifetime of the address pool by less than one month. No owners of these address pools appear to be willing to do this anyway. Therefore, there is a clear indication that no new address blocks could be claimed back. In reality it means that no one, having excess IP addresses, is going to give them back to the community.

Though such measures may provide some interim respite, sooner or later the demand for IP addresses will be too large to be satisfied by the global IPv4 space. Therefore, these are only temporary solutions. **The only long-term solution is IPv6.**

1.5 IPv6: The best way forward

- (i) IPv6 provides a straightforward and long term solution to the address space problem. The number of addresses defined by the IPv6 protocol is huge. IPv6 allows every citizen, every network operator (including those moving to all IP-“Next Generation Networks”), and every organisation in the world to have as many IP addresses as they need to connect every conceivable router, host, network and devices directly to the global Internet.
- (ii) IPv6 was also designed to facilitate features which were not tightly designed in IPv4. Those features included enhanced quality of service, auto-configuration, end-to-end security, built-in multicast and mobility and many others.
- (iii) The benefits of IPv6 are apparent whenever a large number of devices need to be easily networked, and made potentially visible and directly reachable over the Internet e.g. sensor networks.
- (iv) Prompt and efficient adoption of IPv6 offers India potential for innovation and leadership in advancing the Internet. Other regions, in particular the Asian region, have already taken a strong interest in IPv6. For instance the Japanese consumer electronics industry increasingly develops IP enabled products and exclusively for IPv6. The India industry should therefore be ready to meet future demand for IPv6-based services, applications, and devices and so secure a competitive advantage in world markets.

1.6 Advanced Features in IPv6

- a) **Large number of Addresses** – The main reason for designing IPv6 is the shortage of addresses in IPv4. IPv6 has 128-bit addressing. This address space supports a total of 2^{128} (about 3.4×10^{38}) addresses, which has the potential to cater to the addressing needs of enormous number of devices for many years to come. The standard allocation block of IPv6 addresses is a “/48”, which is large enough to cater to the largest organization on earth.
- b) **Address Autoconfiguration** – IPv6 hosts can automatically configure themselves when connected to an IPv6 network by using ICMPv6 messages. This is in stark contrast to IPV4 networks where a network administrator has to manually configure the hosts. Some limited auto configuration facility can be done using

DHCPv4 in IPv4 but this is a very old protocol and has numerous issues and limitations. Therefore, IPv6 is more suitable. When a host is first connected to the IPv6 network, it sends out a *router solicitation* packet for the configuration parameters. Routers will respond with a *router advertisement* packet containing the network layer configuration parameters. The host will then configure itself with the received information. If stateless autoconfiguration is unsuitable then stateful autoconfiguration using a DHCPv6 server can be used.

- c) **Multicast** – The ability to send a single packet to multiple destinations is a part of the IPv6 specifications.
- d) **Mandatory security in network layer** – Internet Protocol security (IPSec) is mandatory in the network layer and is a part of the IPv6 base protocol suite. It is optional in IPv4 and moreover, NAT is so extensively used in IPv4 that IPSec does not work as intended.
- e) **Simplified Router processing** – To simplify the routing process the headers have been redesigned and made smaller for faster processing by routers.
 - (a) In IPv4 main header length is variable but in IPv6 it is fixed length of 40 bytes.
 - (b) Optional functions have been moved to separate extension headers.
 - (c) Routers don't compute checksum, since this is done in the link layer
 - (d) TTL has been replaced by Hop limit
 - (e) On the way routers do not fragment the packets since Path MTU discovery is done by originating router.

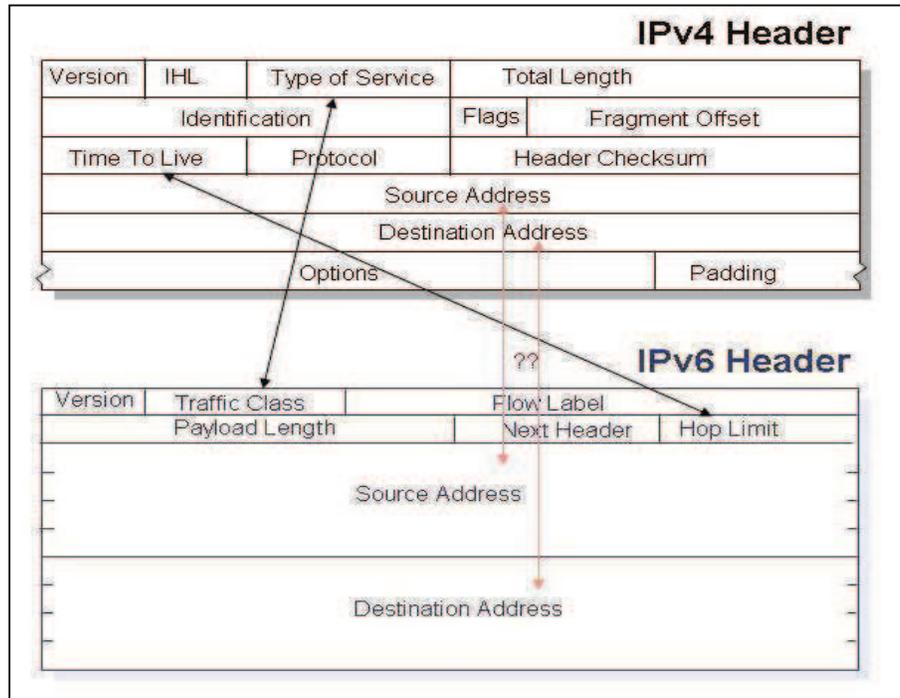


Figure 4: Comparing IPv4 and IPv6 Headers

f) **IP Host Mobility** – For many years the Internet has been used in the pull mode by users, i.e. users request information from the internet. Over the years a new breed of push applications are emerging like stock alerts, sports results, peer-to-peer services like multimedia messaging and voice integration etc, where ISPs have to push these services to a user. But then the ISPs must be able to reach the user always using the same network identifier, irrespective of the point of attachment to the network. IP Host mobility, a new feature, is designed for this need and could be a key driver for deployment of IPv6. Mobile IPv6 (RFC 3775, 3776) enable a mobile node to arbitrarily change its location on an IP network while maintaining existing connections. One of the extension headers is the Mobility Header, used for implementing this function in IPv6. Some practical uses of MIPv6 could be as below –

- (a) **Enterprise on the move** – E.g. courier companies like DHL, FedEx or public transportation like buses, metro, taxis, trucks etc. The nodes are moving during operations.
- (b) **Globally reachable home networks** – In IPv6 the minimum size given to a user is /64. With this addressing space the user can create a home network connecting various devices like surveillance

cameras, fridges, air conditioners and other equipments. These can be accessed and managed through the Internet. When the family moves from one place to another, the whole network can move using IP mobility.

- (c) **Internet enabled transport (cars, buses, trucks etc.)** – Inter-vehicular communication can be made simple using MIPv6. The vehicles can organize themselves into a dynamic mesh network and relaying the packet information amongst themselves, while they are all moving.
- g) **Support for Jumbograms** – IPv4 limits the payload size to 64KB in a packet. This limit is not there in IPv6. Payload size can be as large as possible depending upon the MTU. This can greatly improve performance on high MTU paths.

1.7 Interworking IPv4 and IPv6

IPv6 is not backward compatible with IPv4. IPv4 hosts and routers cannot directly deal with IPv6 traffic. The Internet today is running almost entirely on IPv4. There are IPv6 networks around the world but they are quite scattered. The Internet cannot switch overnight from IPv4 to IPv6. Therefore it is essential that both IPv4 and IPv6 networks are able to talk to each other and the co-existence will be there for years to come. There will be a transition phase (expected to last for many more years). There are 2 operating situations –

- (a) IPv6 nodes have to communicate with IPv4 nodes. This problem is solved using **Dual Stack** technique.
- (b) Isolated islands of IPv6 will have to communicate with each other using the widely available IPv4 networks. This problem is solved using **Tunneling** technique.

1.7.1 Dual Stacking

Nodes with dual IP stacks will have both IPv4 and IPv6 protocol stacks. When communicating with IPv6 nodes they use the IPv6 stack and while communicating with the IPv4 nodes they use the IPv4 stacks. The IPv6 side uses native IPv6 addresses and the IPv4 side uses native IPv4 addresses.

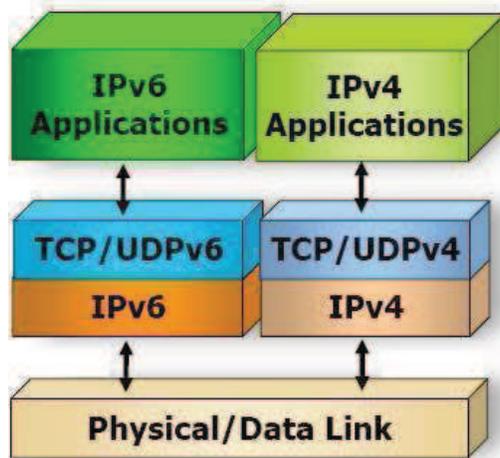


Figure 5: Dual Stack Mechanism

1.7.2 Tunneling

There are several types of tunnels: 6in4, 6to4, Teredo, TSP and others. Some require public IPv4 addresses for each end of the tunnel, some work even behind NAT. Some require manual setup and others are created automatically. In this scheme, one type of packet is encapsulated in another type for transporting. An example is shown below where v6 packets are encapsulated in v4 packets.

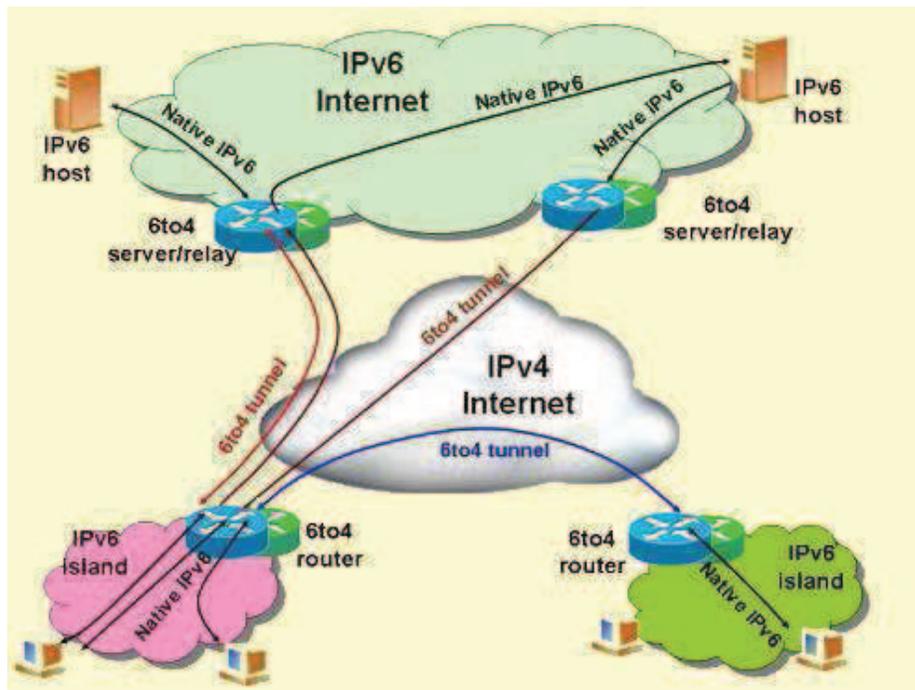


Figure 6: Tunneling Mechanism

1.7.3 Translation

There also exists “translation” such asIVI and NAT64/DNS64. These mechanisms allow translation of IPv4 to/from IPv6 at the IP layer. There are also Application Layer Gateways (ALGs) that can convert IPv4 traffic to/from IPv6 traffic at the Application layer (e.g. for web, email, VoIP, etc).

1.8 Stakeholders in the Transition Process

Because of the universal character of the Internet Protocol, deployment of IPv6 requires the attention of many stakeholders worldwide. The relevant stakeholders in this process are:

- (i) **Internet organisations** (such as ICANN, RIRs, and IETF), which need to manage common IPv6 resources and services (allocate IPv6 addresses, operate domain name system (DNS) servers, etc), and continue to develop needed standards and specifications.
- (ii) **ISPs**, over time, have to offer IPv6 connectivity and IPv6 based services to customers. There is evidence that less than half of the ISPs offer some kind of IPv6 interconnectivity. Only a few ISPs have a standard offer for IPv6 customer access service (mainly for business users) and provide IPv6 addresses.
- (iii) **Infrastructure vendors** (such as network equipment, operating systems, network application software), which need to integrate IPv6 capability into their products. Many equipment and software vendors have upgraded their products to include IPv6. The installed equipment base of consumers, such as small routers and home modems to access the Internet, still by and large do not yet support IPv6.
- (iv) **Content and service providers** (such as websites, instant messaging, e-mail, file sharing, voice over IP). They must be reachable via IPv6. Worldwide there are only very few IPv6 enabled websites, though growing by the day. The de-facto non-existence of IPv6 reachable content and services on the Internet is a major obstacle in the take-up of the new protocol.
- (v) **Business and consumer application vendors** (such as business software, smart cards, peer-to-peer software, transport systems, sensor networks), which

need to ensure that their solutions are IPv6 compatible and increasingly need to develop products and offer services that take advantage of IPv6 features. IPv6 has the potential to enter into new areas such as logistics and traffic management, mobile communication, and environment monitoring which has not taken place to any significant degree yet.

- (vi) **End-users** (consumers, companies, academia, and public administrations), which need to purchase IPv6 capable products and services and to enable IPv6 on their own networks or home Internet access. Many home end-users, without being aware of it, operate IPv6 capable equipment but due to missing applications cannot make use of it. Companies and public administrations are cautious to make changes to a functioning network without a clear need. Therefore there is not much user deployment in private networks visible. Among the early adopters have been universities and research institutions. All EU national research and education networks also operate on IPv6. The European Géant network is IPv6 enabled, whereby approximately 1% of its traffic is native IPv6.

1.9 Some IPv6 Initiatives around the World

1.9.1 CHINA

China instituted a full adoption policy of IPv6 by creating the China Next Generation Internet (CNGI) for completion in 2006. CNGI was conceptualized to become the nationwide backbone to integrate all services in China for fixed, mobile, GRID and research. CNGI has leapfrogged and shortened the gap with developed countries in the Internet development. Now the Internet is developing at a rapid rate in China, which makes it the second largest country in terms of Internet users.

How did CNGI happen ? CNGI can be traced back to the end of 2001. At that time, approximately 57 academics wrote a letter to the leaders of State Council stating that they hoped to construct an academic network of second generation Internet and the position at that time was only an academic network. Later National Development and Reform Commission (NDRC) felt that studying NGI was also mentioned in some other domestic projects, so NDRC organized a strategic experts committee about the Internet development

in August 2002. After half-year's study, they called the project CNGI. Many other issues were also debated but finally after the authorization of major leaders of State Council, this project was then initiated. NDRC is the leading ministry and Ministry of Science and Technology (MST), Ministry of Education (ME), Ministry of Information Industry (MII), the State Council Information Office (SCIO), Chinese Academy of Science (CAS), Chinese Academy of Engineering (CAE) and National Natural Science Foundation of China (NSFC) organize it. It is an **8-ministry driven Inter-ministerial effort**. CNGI has very wide participation from industry and academia. The participants hope that they can explore technologies, cultivate personnel, innovate applications with commercial value, change the non-profitable situation of Internet, do research and bring the fruits of CNGI to future commercial use.

1.9.2 EUROPE

The European Commission has shown strong support for IPv6 with the creation of the EU IPv6 Task Force. They have funded many projects like 6INIT, 6WINIT, 6NET, Euro6ix etc. EU Commissioner Erkki Liikanen endorsed the IPv6 initiative and the first recommendations were worked out followed by the continuation of the Task Force Steering Committee project for phase I and then Phase II. The following European government and national regulators expressed interest to promote IPv6:

- (i) The French Government supported the French IPv6 Task Force forming the largest IPv6 group in Europe.
- (ii) The Spanish government supported the Spanish Task Force and holds currently the coordination of its work.
- (iii) The Austrian government supported the creation of the Austrian IPv6 Task Force primarily to promote IPv6 for increasing broadband penetration. The Austrian IPv6 task Force has declared that IPv6 was the logical missing piece in achieving the objectives set out for broadband.
- (iv) The Finish Regulator Ficora is the host and the leader of the Finish IPv6 Task Force.
- (v) In Portugal, a strategic group was formed in November 2004 to prepare a policy document to have it addressed by the Portuguese Government.
- (vi) The Irish government has appointed Wattford Institute of Technology as the centre of Excellence for IPv6.
- (vii) The Luxembourg government supported the initiative of the chair of the

EUv6TF to design a large scale IP project to research public safety using IPv6 as the underlying protocol which gave birth to the U-2010 project.

1.9.3 JAPAN

The Japanese Government has taken on a program initiative around the concept of ubiquity called “u-Japan” (Ubiquitous Japan) as the 2010 ICT Society platform. It is centred on empowering the Japanese end-user:

- Ubiquitous access, connecting everyone and everything
- Universal and user-friendly
- User-Oriented
- Unique, be something special

The Japanese government is focussing on technologies to make that ubiquity happen from home networks, over 4G networks (skipping 3G) to space communications and from sensor networks to RFID. One of the most important initiatives is promotion of IPv6. It supported the creation of the IPv6 promotion council (v6PC) and created a public-private partnership. The focus of the IPv6 Promotion Council (v6PC) today is on applications with a number of funded projects. They are working on tele-control application, Live E! project⁵, InternetCAR Project⁶, Digital IP-TV multicasting (Japan analog TV is to be shutdown by 2011), Digital buildings. Potential application areas of IPv6 are for Network Service (NGN (Next Generation Networks), FMC (Fixed to Mobile Convergence), Triple Play and Wireless), non computer devices/ embedded devices, Sensors, Buildings safety and security, Energy, Emergency response etc.

Japanese vendors are also actively participating in the IPv6 Ready Logo Program. The net result is that over 30% of the products that obtained the IPv6 Logo are from Japan of the phase-I Logo and 50% of the phase-II Logo.

1.9.4 NORTH AMERICA

The US Department of Defense (DOD) has taken initiative leadership by announcing support for IPv6 back in June 2003 after consultations with the North American

⁵ <http://www.live-e.org>

⁶ <http://www.sfc.wide.ad.jp/InternetCAR/>

IPv6 Task Force and the IPv6 Forum. The military sector also responded favorably for IPv6 support. The DOD has recognised IPv6 as a Key to Net- Centric Combat Operations with a clear call to industry to support the DOD vision to empower the edge, i.e. the soldier:

The North American IPv6 Task Force (NAv6TF) www.nav6tf.org has worked with US Federal Government and with the Office of Management and Budget (OMB). On August 2, 2005 OMB issued a letter setting June 2008 as the date all US Federal Agencies must be using IPv6. The US Department of Commerce has released a very comprehensive IPv6 Final Report. *National Telecommunications and Information Administration has set up an infrastructure for federal departments and agencies to request IPv6 addresses and has set up a working group to further assist in the transition.*

Moonv6 www.moonv6.org is an international project led by NAv6TF to execute deployment testing of IPv6 technology. It is jointly implemented by commercial service providers, UNH- IOL, Government organizations, academic entities and network equipment vendors. Test items are determined by network operation requirements of the US Government Agencies and commercial service providers.

NAv6TF also started the Metronet6 project which is an emergency responder network concept built using IPv6. It is a 24x7x365 ad-hoc mobile network that integrates E911, Internet, and voice on a common IPv6 infrastructure. The technology has capability to support multiple simultaneous deployments from a central infrastructure.

1.9.5 SOUTH KOREA

South Korea initiated its IPv6 journey in Feb 2001. The Government started promotion of IPv6 by devising a new platform called IT839 selecting 8 services, 3 infrastructures and 9 growth engines. Boosted by government support and early adoption by communication carriers, domestic equipment makers, large and small, and research organizations accelerated development of equipment needed for deployment of the next-generation Internet address system.

As part of their IT839 strategy, the Ministry of Information and Communication implemented first phase pilot project of KOREAv6 in 2004, and it conduct the second phase pilot service in 2005 to foster adoption of IPv6 technologies and energize the new communication service. **The South Korean public sector has been engaged in deploying IPv6 on national level by building a nation-wide IPv6 MPLS backbone.** IPv6 has been deployed in 2004 in the e- Government networks, the postal office, universities, schools, ministry of defence, local governments, etc.

1.9.6 TAIWAN

Taiwan has implemented its policy by announcing their e-Taiwan program, designed by the National Information and Communication Initiative Committee. The program calls for a complete package to address e-Society, e-Commerce, e-Government and e-Transportation with the announcement to make Taiwan the most advanced nation in Internet technologies.

The Taiwan National IPv6 Program addresses all aspects which is a concerted effort between industry and Government. The IPv6 program office sits at the heart of the equation and gets full authority to define policies and promotion plans. The most formidable announcement of the e-Taiwan initiative was the plan to have 6 Million Broadband end-users by 2008 using IPv6. The government networks were ready to use IPv6 by 2007.

Examples of countries given above show that interest and push from the government has pushed the cause of IPv6 forward in their respective countries.

1.10 Maintaining India's competitiveness and development in the country

Various large service providers in India have obtained IPv6 addresses from APNIC. Smaller service providers usually obtain their addresses from the upstream service providers. Large service providers are in various stages of implementing IPv6 and some of them have committed that they would complete the transition process before the exhaustion of IPv4 addresses. However, most of the small and medium scale ISPs are not prepared for transition as they are dependent on their upstream larger service providers in the chain and once the larger service providers migrate to IPv6 they shall also follow them.

Today, for most stakeholders the advantages of adopting IPv6 are not immediately visible. The benefits are long-term and also depend on other stakeholder's decisions on when and how to implement IPv6. The more users work with IPv6 the more attractive it becomes for others to do the same. As the number of users increases more products and services will be offered at lower prices and better quality. This is a situation, which can be improved by appropriate policy measures and give the market a stimulus by encouraging people and organisations to consider moving ahead positively. Those measures will be more effective when taken collectively at country level.

VSNL (Tata communications) owns and run one of the largest international backbone networks, all of which is already fully dual stacked (this was acquired in the purchase of Teleglobe Canada). Some of the other organizations like NIXI and ERNET have carried out activities in India. NIXI is setting up parallel IPv6 Exchange Routers in Mumbai and Delhi, Dual Stack Routers in Mumbai, Delhi(Noida), Chennai and Bangalore. NIXI has started taking IPv6 addresses in database of .IN Registry for resolving website hosted with IPv6 Addresses. NIXI has applied to APNIC for becoming National Internet Registry-where IPv4,IPv6 Addresses and AS number will be allocated to Indian members by NIXI and APNIC has agreed in-principle. Similarly ERNET backbone has been upgraded to provide dual stack access of IPv6 and IPv4 to its users to develop, test and implement IPv6 based mail, DNS, web applications and products. The Indian Institute of Science, Bangalore (IISc) has also set up a testbed in association with 6Choice EU project, in their campus in Bangalore . They use this testbed to provide hands-on training to different stakeholders.

The details of various activities carried out by TEC in India and the readiness of service providers is given in subsequent chapters

1.11 Objective of this Document

The objective of this document is to propose practical recommendations to support the widespread introduction of the next version of the Internet Protocol (IPv6) in India with following reasons –

- (i) Timely implementation of IPv6 is essential as the pool of free IP addresses provided by IPv4 is being depleted down to just 6% and expected to run out by mid-2012.
- (ii) For successful transition, it is necessary to coordinate the efforts of a large number of stakeholders like service providers, educational institutions, government departments, private organizations, industry associations etc. In fact anyone, who is associated with Internet, either as a user or a provider, has to be involved in this process.
- (iii) To set India in a leadership position in the New Internet Economy sustaining its competitiveness in the global economy
- (iv) To set the stage for innovations and future Internet content and services based on two-way and interactive Internet paradigm

-----x-----

	2
--	----------

**IPv6 initiatives in
India by
Telecommunication
Engineering Centre
and DoT**

2.0 Policy decisions taken by DoT

In early 2004, Migration from IPV4 to IPV6 in India was listed as one of the items in the Ten Point Agenda given by Hon'ble Minister of Communications & Information Technology. After due deliberations a Committee under the Chairmanship of Advisor(T), DoT was formed in DoT vide letter no. 813-7/05-LR(Vol.II) dated 24.05.05 with the following objectives –

- Roadmap to achieve transition from IPV4 to IPV6, clearly bringing out the steps involved
- Financial implication for BSNL & MTNL

After due deliberations on the issue, the Committee submitted its report in August 2005. At the same time, in August 2005, TRAI also issued its consultation paper on migration from IPV4 to IPV6. The report of the Committee was examined in DoT and decisions were conveyed by DoT letter no. 813-7/2005-LR(Vol.II) dated 22nd April, 2009. Additional decisions on TRAI recommendations were also issued by DoT. **For facilitating the migration from IPV4 to IPV6, TEC was mandated by DoT to takeup certain activities as described below-**

- (i) To take up with telecom equipment manufacturers and service providers to deploy IPv6 compliant equipments in the country.
- (ii) To take up the matter with telecom equipment manufacturers for indigenous development and production of IPv6 compliant equipments.
- (iii) Organizing workshops throughout the country for awareness.
- (iv) Firming up the transition plan for the country in consultation with different stakeholders.
- (v) Creation of task force
- (vi) Take up with different government departments for appointment of nodal officers to form their transition plans in consultation with TEC
- (vii) Conduct/ arrange training programmes for imparting knowledge skills in IPv6 domain.

In accordance with above mandate to TEC, discussions were initiated with industry members and service providers, and it is emerged from all these discussions that, in addition to other activities, workshops be held with all Telecom Service Providers, Equipment Manufacturers and all concerned stakeholders for IPV6 awareness and firming up the transition strategy. Since it was important that industry associations and their members should be sincerely involved, agreement was reached with CMAI, an industry association closely associated with many other telecom industry associations like TEMA, AUSPI, COAI, ISPAI, Wimax Forum of India, CTIA etc. for conducting the workshops in PPP mode. Accordingly the following workshops were conducted by TEC in association with CMAI and IPV6 Forum

2.1 Telecommunication Engineering Centre (TEC)

It is a technical wing under the Department of Telecommunications, Government of India which is entrusted with the following activities –

- (i) Development of Specifications for common standards with regard to Telecom network equipment, services and interoperability.
- (ii) Preparation of Generic Requirements (GRs), Interface Requirements (IRs) and Service Requirements (SR) documents for different types of telecom products and services.
- (iii) Issuing Interface Approvals and Service Approvals.
- (iv) Formulation of Standards and Fundamental Technical Plans.
- (v) It also interacts with multilateral agencies like APT, ETSI and ITU etc. for standardization.
- (vi) It also develops the expertise to imbibe the latest technologies and results of R&D.
- (vii) It provides technical support to DOT and technical advice to TRAI & TDSAT.
- (viii) It coordinates with C-DOT for the technological developments in the Telecom Sector and for policy planning by DOT .
- (ix) It has also been mandated by the DoT as the nodal agency in India to coordinate all IPV6 related activities in the country.

2.2 Workshops Conducted by TEC

1. First workshop with CMAI held on 21st July 2009, Hotel IIT, New Delhi

The first full day workshop organized jointly by TEC and CMAI and IPv6 Forum as Knowledge Partner was held in New Delhi on 21st July 2009. The theme of the workshop was “**Migration from IPV4 to IPV6 in India**” It was attended by about 250 participants from different organizations including Service providers, Software Industry, Central government departments/ministries, State governments, PSUs, Educational Institutions etc. The workshop was inaugurated by Shri. Siddhartha Behura, then Secretary(T), DoT. The other distinguished guests were Shri V.K.Shukla, Member(Technology), DoT; Shri R.N.Prabhakar, Member(TRAI) ; Shri K.Sridhara, former Member(Technology), DoT; Shri D.K.Agrawal, Advisor(Technology), DoT; Shri R.K.Arnold, Secretary(TRAI) and Shri N.K.Srivastava, Sr.DDG(TEC).

There were speakers from BSNL, MTNL, TRAI, Bharti Airtel, Tata Communications Limited, COAI, Tata Teleservices Limited, SIFY, DoT, TEC, Orange Business Services, M/s 3Com and IPV6 Forum India.

Certain actionable points emerged from the first workshop, which are given below.

- (i) **More such workshops are needed** - 5 were planned in the financial year 2009-10.
- (ii) **Future procurement of IPV6 compliant ICT equipments** - Secretary(T), DoT has written to Secretaries of different Central govt. ministries and Chief secretaries of the state governments, vide letter dated 03rd September 2009 for making necessary arrangements by subordinate departments and organizations for procuring only IPV6 compliant ICT equipments for all new procurements in future and have an action plan for the replacement of IPV4 network/devices in a phased manner.
- (iii) **Appointment of nodal officers in different Central and State Government departments** – The Department has also written to all Secretaries and Chief

Secretaries of Central and State Govt. departments for nominating nodal officers for coordinating with TEC for transition to IPV6.

- (iv) **Firm transition plan for India** – TEC will prepare the National transition plan in consultation with all stakeholders.
- (v) **Standardization of IPV6 equipments** - TEC is focusing on the requirements of IPV6 compatible Telecom Products and it has issued the TSTP (Test Schedule and Testing Procedure) and circulated among various stakeholders for comments. Based on comments received these procedures shall be reviewed and refined and thereafter it shall be complied by all concerned.
- (vi) **Signing MoUs and Agreements** – IPV6 Forum India is the Indian chapter of the Luxembourg based International organization “World IPV6 Forum”. It was envisaged to leverage their expertise on IPV6 deployment in other countries in the world. So, TEC has entered into an MOU with the IPV6 Forum for their various programmes in the country.

2. Second Workshop with CMAI held on 15th September 2009, Indian Institute of Science, Bangalore

The second full day workshop with CMAI and technical support of the IPv6 Forum was held on 15th September 2009 in the Indian Institute of Science, Bangalore. The theme was “**IPV6 Transition and Greenfield Applications in India**”. The workshop was inaugurated by Shri D.K.Agrawal, Advisor(technology), DoT and Prof. N.Balakrishnan, Associate Director, IISc was the Guest of Honour for the event. Around 240 delegates from different organizations participated. In the workshop Greenfield applications like Intelligent Transport Management System, Sensor Networks to save energy in buildings, Cloud Computing, Internet Data centers, Scalable Cable TV networks were discussed. There were speakers from TEC, IISc Bangalore, IPV6 Forum, BSNL, M/s 3Com, M/s Tech Mahindra, M/s Spectranet, M/s Tata Communications Limited, M/s Qualisystems, M/s CISCO, M/s Juniper and M/s Hewlett Packard India. The discussions in the workshop were summarized by Shri. N.K.Srivastava, Sr.DDG, TEC

The following actionable points emerged from the 2nd workshop –

- (i) **Pilot Projects** - Promoting Pilot Projects in Greenfield Applications using IPV6 with support from Government. IIT Kanpur is preparing a concept paper on “**Intelligent transport System**”, which can be implemented in association with BSNL.
- (ii) **IPV6 task force** – There is need for an IPV6 task force which will be represented by different stakeholders from industry and government. The members of the task force will work together to facilitate transition to IPV6 in the country.
- (iii) **IPV6 trainings in association with APNIC, Australia** – APNIC representative also came to attend the IPV6 workshop in Bangalore. It was discussed how TEC can collaborate with APNIC for IPV6 trainings in the country. The first such TEC/APNIC joint IPV6 training was held on 25-26th November 2009 in Mumbai.

3. **Third Workshop with CMAI in Chennai on 22nd October 2009**

The third workshop was held on 22nd October 2009 in Chennai. The theme of the workshop was “**IPV6 as a New Platform for Innovation**”. There were about 200 participants from different organizations. The workshop was inaugurated by Shri Chandra Prakash, Member(Technology), DoT. Other distinguished guests on the dias were Shri. D.K.Agrawal, Advisor(T), Dr. Bhaskar Ramamurthy, IIT Chennai, Shri. N.K.Srivastava, Sr.DDG, TEC and Shri P.W.C. Davidar, Secretary(IT) Tamil Nadu State and Shri N.K.Goyal, President CMAI in the event. In the workshop innovative applications involving IPV6 were covered in great depth by various speakers on subjects like **Intelligent Transport System, Sensor Networks to save energy in buildings, IPV6 based emergency response systems** etc. There were speakers from APNIC, DoT, TEC, DIT, IISc Bangalore, IIT Kanpur, IPV6 Forum, Tech Mahindra, M/s Tata Communications Limited, M/s CISCO. The speaker sessions were chaired by Shri. Baskar Ramamurthy from IIT Chennai and Shri. Ram Narain, DDG(Security), DoT.

There was also a lively panel discussion on “**IPv6 as a New Platform for Innovation**”, which was chaired by Shri. R.M.Agarwal, DDG(SA), TEC and Co-chaired by Shri. B.K.Nath, Dir(SA), TEC . It was attended by Shri Hemant Dattatreya of the IPv6 Forum, India and others.

The following actionable points have emerged from this workshop.

- (i) **Committees for different works** – The task force which will be formed by different stakeholders will have different committees for different works related to IPV6 implementation in the country.
- (ii) **Separate workshop for nodal officers** – TEC will organize a separate workshop for nodal officers in different Ministries and state government departments to educate them on IPV6 as well as preparing transition plans with their consultation.
- (iii) **Checklist for IPV6 compliance** – TEC shall prepare a checklist for IPV6 compliance and circulate to all concerned.
- (iv) **More trainings in association with APNIC** – Training sessions on IPV6 implementation are needed throughout the country and TEC shall associate with APNIC for conducting more such trainings in India.

4. IPV6 hands-on training by Asia Pacific Network Information Centre (APNIC) in association with TEC and support of CETTM, MTNL Mumbai.

A two day IPv6 hands-on training programme from 25th -26th November 2009 was organized by TEC in association with Asia Pacific Network Information Centre (APNIC), headquartered in Australia and CETTM MTNL Mumbai. The training was organized by TEC as part of its activities to create a pool of trained manpower in IPv6 in different organizations. It was inaugurated by Shri J.Gopal, Executive Director, MTNL Mumbai. To impart the training, 2 trainers (Mr. Srinivas Chendi and Mr. Champika Vijayatunga) had come from APNIC, Australia. The entire training infrastructure and other facilities were provided by CETTM, MTNL Mumbai. The training was attended by 35 participants belonging to different organizations. At the end of two-days training certificates were distributed to the participants by APNIC. **It emerged from discussions later on that more such training programmes have to be organized and CETTM, MTNL Mumbai has shown keen interest to co-host the training events.**

5. The Fourth workshop with CMAI on migration from IPV4 to IPV6 in India was held on 27th November in Mumbai.

The fourth full day workshop was held on 27th November 2009 in Mumbai. The theme of the workshop was **“IPV6: New Opportunities for the Country”**.

There were around 150 delegates from different Central Government Departments, State government departments, Industries, Service Providers, Educational Institutes, Public Sector Undertakings etc. There were also delegates from the Cabinet Secretariat, Defence Ministry and Home Ministry among others. It was inaugurated by Shri Chandra Prakash, Member(Technology), Department of Telecommunications. Shri N.K.Srivastava, Sr.DDG, TEC in his speech mentioned about the various activities of TEC and also that TEC has entered into an MOU with the IPv6 Forum to leverage their International Expertise for deployment of IPV6 in India.

In the workshop there were different sessions in which presentations were given by national and international speakers from many organizations like APNIC, 6Choice Project, IISc,, IIT Mumbai etc. These sessions were chaired by Shri Jai Chandra, President IPV6 Forum India and Shri Nitin Jain, DDG(DS), DoT. Sh. Jai Chandra, IPV6 Forum mentioned that adoption of the actionable points by various Govt. Depts. can take India a big way forward. Mr. Nitin Jain, DDG(DS), DoT in his remarks said that IPv6 protocol is more secure than the IPv4 protocol.

There was also a panel discussion on “Adopting *IPv6: A New way Ahead*”. The panelists were Dr. Govind from DIT, Mr. German from APNIC, Sh. Jai Chandra from IPV6 Forum India and Sh. Badrinarayan from Tata Communications. The panel was chaired by Shri R.M.Agarwal, DDG(SA) and co-chaired by Shri B.K.Nath, Dir(SA-III) from TEC. **It emerged from the panel discussion that the Government should mandate the transition from IPV4 to IPv6 in a time bound manner by all concerned, seeing the projected timeline for IPv4 Exhaustion.**

The following actionable points have emerged from this workshop –

- (i) **IPv6 Ready Logo Programme** - Since TEC has already signed an MOU with the IPV6 forum it shall leverage this MOU to bring the IPV6 Ready Logo Programme to India for testing and certification of IPV6 compliant equipments in India. This is necessary so that Indian manufacturers need not go abroad for certification of their equipments.
- (ii) **Checklist, Guidelines and Transition Plan** - A model checklist and guidelines along with a generic transition plan has been prepared for various organizations and government departments, which was distributed as a pamphlet in the event.

This was subsequently issued to all nodal officers. A copy of that checklist is also enclosed as Annexure-A.

(iii)**Pilot Projects** - A number of possible pilot projects which can be deployed using IPv6 were discussed in the workshop. It is possible for each government department to take up one such pilot project. The Department of Telecommunications will take up with different ministries and departments of the state and central government for implementing such pilot projects.

(iv)**Creation of Task Force** – Structure of various working committees under the Task Force was discussed and nominations were called for from different stakeholders.

6. One International Summit was also organized jointly by the IPv6 Forum and TEC in New Delhi on 15-16th December 2009. In this summit there were speakers from both India and abroad. It was attended by dignitaries like Latif Ladid, President World IPv6 Forum; Paul Wilson, Director General APNIC; Martin Levy, Hurricane Electric USA; Hiroshi Miyata, WIDE Project Japan; Lawrence Huges, CEO Infoweapons, Phillipines etc. amongst others. It was inaugurated by Shri Chandra Prakash, Member(T), DoT and attended by Shri D.K.Agrawal, Advisor(T), DoT and Shri N.K.Srivastava, Sr.DDG(TEC). The prominent speakers on day-1 were Shri N.Ravishanker, Joint Secretary, DIT and Shri R.M.Agarwal, DDG(SA), TEC in addition to others. On the 2nd day of the summit there was a panel discussion on “**Mandate for IPv6 deployment**” chaired by Shri Subodh Kumar, Additional Secretary, DoT. The panel discussion was attended by various members like Mr. Latif Ladid President IPV6 Forum; Mr. T.R.Dua, Deputy Director General, COAI; Mr. Naresh Ajwani, Secretary ISPAI; Mr. Anil Prakash, Secretary General, IPTV Forum and Mr. S.N.Jindal, Director General ACTO. The comments put forth by various panelists are given below –

- i. Indian businesses are driven by volumes and population. As per the DoT report there are 500 million mobiles and expected to be 1 billion by 2014. There are 1273 cybercafe seats and 50 million PCs. However, the use of IPv6 is <1% and very little traffic flows. Everyone is looking to build a business case based on volumes and hence the slow takeup of IPv6.

- ii. Main challenges in IPV6 deployment are –
 - a. Lack of perceived business need
 - b. Lack of users
 - c. Cost Implications – India is a very cost conscious country and It is not very clear what are the costs involved in transition. Service providers will have to work it out on their networks.
 - d. It is difficult to impose business cases on people unless government gives subsidies or make use of the USO Fund for pushing IPV6 deployment. It was also commented that looking at the scenario in India, firm timeline is required.
- iii. President IPv6 Forum commented that both India and China have shown excellent progress in mobile penetration. But when it comes to Internet users, there are 300 million in China and only 50 million in India. This vast difference shows that the Internet Model is broken in India. Not only India, the US and the Australian models are also broken. The US is trying to fix their model with a new broadband policy. He also mentioned that there are 3 types of deployment models followed by different countries –
 - a. **Business model** – In this model the customers will pay for the transition.
 - b. **Public Interest Model** – Here the governments have a progressive outlook and take keen interest and they use the taxpayer’s money to build the infrastructure.
 - c. **Laggards model** - In this model both the governments and the industry follow the wait and see policy. Looking at the deadlines India may not be prepared to handle a disaster using a laggard’s model.
- iv. It was also commented that there was a **market failure** in case of IPv6 deployment in India. Therefore the government will have to step in.
- v. One question from audience was on the likely scenario when IDN (Internationalized Domain names) would be implemented. It was pointed out by Mr. Latif that deployment of CCTLD in 22 languages in

India would lead to a jump in localized content (hence DNS entries) leading to further demand for IP addresses. Having a DNS without an IP address is useless because each DNS needs an IPv4 / IPv6 address.

vi. **Suggestions Crystallized from the discussion** – Additional Secretary, DoT summarized the discussions in the following points-

- a. It was agreed that India must not follow the Laggards Model. Both the government and the industry should take active interest in deployment of IPV6 in India.
- b. Demand of support from the USO Fund for IPv6 deployment was not yet feasible because it was meant for rural areas. However, it could be thought of if deployment of IPV6 could influence rural teledensity or broadband penetration.
- c. There is also a need to create facilities for testing and certification activities in the country.
- d. Mandate on implementation of IPV6 by service providers is not feasible at the moment because DoT has asked all service providers to submit their transition plans by 31st march 2010. Once the transition plans are received a time frame can be worked out and a need to mandate can be thought upon.
- e. Creation of task force for coordinating the IPv6 deployment efforts was a welcome step and this will be very helpful in sorting out the issues through this common platform and it will be hoped that this will speed up deployment.

7. Fifth full day workshop with IPv6 Forum was held on 22nd January 2010 in Kolkata.

The theme of the workshop was “**IPV6 Migration Timeframe by Consensus or mandate**”. There were around 130 delegates from different Central Government Departments, State government departments, Industries, Service Providers, Educational Institutes, Public Sector Undertakings etc. It was inaugurated by Shri

D.K.Agrawal, Advisor(Technology), Department of Telecommunications. The other important dignitaries who attended the workshop were Shri J.K.Roy, Executive Director(CA),BSNL Corporate Office as Guest of Honour, Shri N.K.Goyal President CMAI, Shri. Rajesh Chharia, President ISPAI; Shri Jai Chandra President IPv6 Forum India and Shri N.K.Srivastava, Sr.DDG(TEC). There was also a panel discussion on “IPv6 Migration Timeframe by Consensus or Mandate”, which was chaired by Shri. R.M.Agarwal, DDG(SA), TEC and co-chaired by Shri. B.K.Nath, Dir(SA), TEC.

The following actionable points emerged from this workshop –

- (i) **Creation of a transition pipe by the government** – Government has to take initiatives in building a transition pipe into which other service providers will connect their IPV6 based networks for exchange of traffic.
- (ii) **Creation of Task Force on priority** – It is important to create the task force on priority to coordinate and take up different activities for IPv6 deployment in the country.
- (iii) **Free IPv6 addresses to applicants** - It was suggested that deployment of IPv6 can be made faster by allocating free IPv6 addresses to the applicants.
- (iv) **Minimise upgradation cost from IPv4 to IPv6** – It was also suggested by some delegates that equipment vendors should not be allowed to charge for upgradation from IPv4 to IPv6. Though, it may not be feasible for free upgradation but equipment vendors can be asked to minimize their upgradation costs.
- (v) **Mandatory IPv6 readiness for govt. procurements** - Govt. can take some steps to mandate IPv6 in certain areas like Govt. tenders and Request For Proposals(RFPs) can make IPV6 readiness of service providers and suppliers mandatory before placing orders on them

2.3 Summary of Outcome of the TEC Workshops and Other activities of the Government

Through all these workshops and other activities, the government has tried to create the required momentum for involvement of different stakeholders. Some of the major inputs, TEC received through these workshops and addressed in this document are summarized below -

- (i) Suitable policy framework by Govt. For smooth transition.

- (ii) The more delay happens, the more expensive it will become.
- (iii) Specific deadlines for transition like other countries (proposed Sept-2011)
- (iv) Creation of IPv6 Task Force and working groups.
- (v) Promoting Pilot projects in “Greenfield Applications” with USO support in specific cases (e.g. Rural Emergency Health care)
- (vi) More Training and awareness activities
- (vii) Guidance to small and medium service providers and organizations on implementing IPv6
- (viii) Asian countries Specially India should not follow the western countries example. (Consensus vs Mandate)
- (ix) From Panel Discussion “**Adopting IPV6: A New Way Ahead**” It emerged that Govt. Should mandate the transition from IPv4 to IPv6 in a time bound manner seeing the projected timelines for IPv4 exhaustion.
- (x) Service providers want a separate “Transition Pipe” for facilitating the connection of isolated IPv6 networks
- (xi) Govt. departments should take IP-based services from only IPv6 ready Internet service providers after a certain period of time (**Leading by Example**)
- (xii) Wait and Watch Policy by some operators, which is not good.

-----X-----

	3
--	----------

**Transition
Plan for
Government
Departments**

3.0 Introduction

The role of the government departments is very crucial for success of IPv6 in India. The government is a very large user of Information Technology products and services. E-services are becoming an increasingly important way for governments to interact with their citizens, from tax returns to voting - effectively they are reshaping the relationship between the elected official and the citizen. The availability of a significantly larger pool of addresses will ensure that government departments are not limited in the roll out of increasingly innovative and citizen-centric service.

3.1 Steps : Government Departments/Organizations can follow

Given the imminent depletion of IPv4 addresses, increasing awareness of the consequences and the importance of IPv6 take-up are essential. While there is no one model of engagement for government departments, there are instances to indicate that different governments throughout the world have taken more or less similar steps as listed below

- a) **First step : Reaching out to stakeholders.** This has been done through engaging both with telecom service provider including Internet community and the industry. Governments has set up multi-stakeholder advisory groups on IPv6 (in some cases, asking them to produce or contribute to national action plans). Finally, governments are also undertaking internal IPv6 assessments to establish the scale of the task of enabling their networks.
- b) **Second step :Leading by example.** Governments are putting a section or organization in charge of the issue, and ensuring that it is endowed with sufficient authority to elicit cooperation from other departments and concerned stakeholders. They are also establishing reporting criteria or measurements. They are setting up working groups to respond to the issues, particularly with regard to ensuring the continuity of government services in the transition to IPv6 and starting to undertake network transition, either on a departmental or agency basis.
- c) **Third is persuasion.** Once it is decided that IPv6 is important then it becomes a matter of communications and persuasion with all stakeholders. Governments have found that declaring that IPv6 will play an important part in the future of their activities and business and its adoption at the earliest possible is in their interest only.

- d) Some governments have gone further and also implemented **non-monetary incentives**, in the form of public procurements requirements related to IPv6, and **monetary incentives** in the form of investments in research into networks, applications, and test beds that use IPv6.

No matter what engagement model that is adopted, clearly the critical first step is to reach out to and engage with relevant stakeholders, to understand the issues and state of play. Governments can specifically help address two of the key challenges (i) **general awareness** and (ii) **the slow take up of IPv6**. Raising awareness of the importance of IPv6 and seamless global addressing to service continuity and national economy is essential. Governments are well placed to communicate to key stakeholder communities about the importance of IPv6 to economic growth, a flourishing digital economy and stable and evolving government to citizen services and outreach. Governments can also lead by example and step up and implement IPv6 within their own networks and organizations.

3.2 Management Structure for IPv6 Deployment in Government departments

For the implementation of IPv6 in Government departments, the first thing that the heads of ministries, departments and different government departments must clearly understand is that the progress of the country is based on effective delivery of public services through widespread deployment of e-governance infrastructure. The e-governance infrastructure that we build today or tomorrow must be robust, scalable and should also not become obsolete very soon. IPv6 is one crucial component of that e-governance infrastructure, which will ensure this.

- 1) To achieve these objectives, it is important to identify concerned persons in these organizations. A clear definition of the roles will allow them to concentrate on their task and deliver quality results at the end of the day. They will have to interact with other government agencies, content developers, software and entertainment companies, research center, technical bodies etc. to ensure that the IPv6 technology is fully utilized and is beneficiary to the end users i.e. the public.
- 2) Planning and execution of the government-wide adoption of IPv6 requires close coordination and cooperation among all the Ministries, departments and the subordinate organizations.

3.3 Appointment of Nodal Officers

The Department of Telecommunications has already written to all central and state government Ministries and departments for the appointment of nodal officers. TEC has received the nominations from many of them and more are still coming. However, it is important that all Ministries, departments and subordinate PSUs appoint at least one nodal officer to coordinate with Central Nodal Agency (i.e. DoT/TEC) for this purpose.

3.4 Functions of the Nodal Officers

- i) The nodal officers shall build a cross-functional team of qualified persons within the department to facilitate the deployment of IPv6. The team will support IPv6 transition planning and implementation, including representatives from various lines of business, infrastructure, application development, security, enterprise architecture, capital planning, budgeting and procurement. The team will receive active guidance from the nodal officer through all phases of the transformation effort. A typical cross-functional team can be as given below –

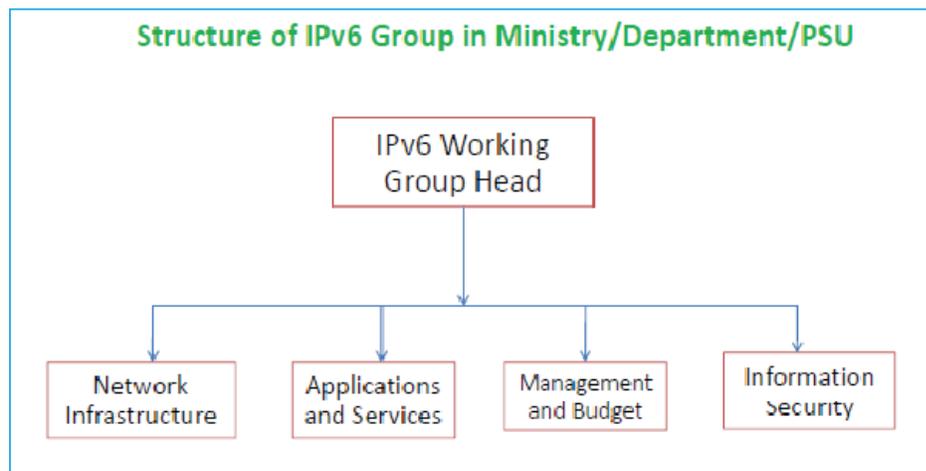


Figure 7: Structure of IPv6 Group in Ministry / Department / PSU

- ii) The concerned nodal officers along with their team will prepare a transition plan for their respective departments/organizations.
- iii) The nodal officers shall have to pursue with the respective service providers and equipment vendors to obtain the status of the network while preparing the transition plan.
- iv) The nodal officers shall be required to get the budget for implementing the plan.

- v) The nodal officers shall also have to coordinate with different application and content service providers to make the applications and content IPv6 compliant.
- vi) The nodal officers shall coordinate with TEC/DoT for all matters related to deployment of IPv6 and for seeking any guidance in this regard.
- vii) The nodal officers may also represent their department in the appropriate body in the “India IPv6 Task Force”, which is under formation.

3.5 Issues that need to be addressed by the departmental cross-functional team during transition

- a) To highlight ways for IPv4 and IPv6 co-existence
- b) To address the potential security risks during the transition
- c) To state the deployment technique or a combination of techniques to be used for the transition to IPv6
- d) To highlight the issues faced or stress factor during the transition process
- e) To ensure that the deployment of IPv6 is minimally disruptive to the operations of the existing networks and devices

3.6 Issues that need to be addressed in the Departmental transition plan

- a) To provide a detailed analysis of risk management and assessment
- b) To ensure that the transition plan is scalable
- c) To list out the costs of transition for the planning process
- d) To identify the applications and equipments that need to be upgraded or replaced
- e) To identify the effects of transition to IPv6 on applications and networks
- f) To allocate the needed resources for the transition plan

3.7 Recommended Phase wise IPv6 Implementation by the Government Departments

The coexistence deployment will be split into 3 phases. It is divided into different phases so as to simplify managing and debugging issues that may crop up along the way. The objectives of the phases are outlined as follows:

- (a) **Phase 1** is targeted at getting the organization's HQ and main office capable of supporting IPv6 and achieving secure global connectivity.

- (b) **Phase 2** is targeted at getting the Regional and other offices of the organization to support IPv6, achieving secure global connectivity.
- (c) **Phase 3** is targeted at migrating primary applications to maximize the features of IPv6.

3.7.1 Phase 1

The objective of Phase 1 is to get the HQ and the main Office of the organization to be able to support IPv6 and achieve secure global connectivity. In order to achieve this objective, the following task needs to be done:

- (a) Plan the budget, network architecture and other considerations.
- (b) Set up a pilot network.
- (c) Perform a comprehensive compliance and security audit.
- (d) Set up few applications to take advantages of IPv6.
- (e) Evaluate the implementation.

3.7.1.1 Plan the budget, network architecture and other considerations

- (a) Budgeting is the biggest concern as one would have to justify costs for newer hardware or software (if needed). This is also where each organization has to identify a business need for IPv6. Some questions that can be asked are:
 - (i) How can IPv6 benefit the organizations?
 - (ii) What are the technical benefits of IPv6 for the organizations?
 - (iii) What business areas can be expanded using IPv6?
 - (iv) What is the impact of IPv6 adoption within the organizations ?
- (b) During the various workshops conducted by TEC, a question was often raised by the participants to know about the approach they have to take to start the transition from IPv4 to IPv6. Earlier, TEC had circulated a checklist giving the basic activities that they have to do. A copy of the checklist is placed at **Annexure-A**. An additional checklist is also enclosed at **Annexure-B**, which can be used for assessment of Network Infrastructure. Organizations can use these checklists to gather information about their current network infrastructure and to identify IPv6 compliance for existing network devices, software and services.

- (c) Once a solid business case to migrate to IPv6 has been identified, departments can begin to:
- (i) Plan the costing for purchasing of newer hardware or software (if needed).
 - (ii) Re-evaluate the network infrastructure to support IPv6.
- (d) It has to be made aware that existing implementations will affect the pace of transition. For instance, some applications in use may be custom written and the vendor may no longer be supporting it. Some applications may even be sending the IPv4 address in the data stream which will affect its usage in an IPv6 environment. These questions and issues should already be known during the making of the pilot network. These issues will determine the cost and time taken to implement IPv6.
- (e) Knowing the products road map is beneficial as some of the hardware or software may already be deemed “end-of-life” or “end-of-service” and the replacement has to be identified before making decisions.
- (f) Organizations should also consider the transition mechanisms that will be used to ease the transition process. **Appendix-C.** can be used to identify the transition mechanisms. This will undoubtedly affect how the entire network is planned and deployed.
- (g) Assuming an organization decides not to use any transition mechanism, the organization will be incapacitating itself as IPv6-only nodes will no longer be able to communicate to IPv4-only nodes. The best and recommended approach is to use the dual-stack mechanism as it provides compatibility for both protocols. The tunneling mechanism can be considered if there is no native IPv6 support in between networks.
- (h) It would also be prudent to consider appointing consultants who would be able to guide and probably share their experience in deploying IPv6. When deploying new technologies, it's always best to seek out those with experience to minimize problems in a production environment. Even with the experience gained from training and the pilot network, there are still unknown issues and bugs that might be available due to inexperience.
- (i) Once a working plan has been identified, the organizations can approach the ISP to obtain a global IPv6 prefix. There are three methods available to assign IPv6 address to end nodes which are:

- a. **Stateless autoconfiguration** – It is also described as “serverless.” Here, the presence of configuration servers (DHCP) to supply profile information is not required. The host generates its own address using a combination of the information that it possesses and the information that is periodically supplied by the routers. Routers determine the prefix that identifies networks associated to the link under discussion.
- b. **Stateful configuration** – It requires a server to send the information and parameters of network connectivity to nodes and hosts. Servers maintain a database with all addresses allocated and a mapping of the hosts to which these addresses have been allocated, along with any information related to all requisite parameters. In general, this mechanism is based on the use of Dynamic Host Configuration Protocol version 6 (DHCPv6).
- c. **Manual configuration** – IPv6 address are manually assigned to the hosts and nodes by the administrator.

3.7.1.2 Set up a Pilot Network

- (a) After acquiring the knowledge about IPv6, each department is encouraged to try out IPv6 and the best way to do this is by creating IPv6 Pilot Networks within the department in few non-core areas. A Pilot Network allows the creation of a scaled down version of the organizations’s production network. It offers each organizations an insight into how introducing IPv6 will affect their network. Additionally, it allows the technical support personnel to apply all they have learned in the training in a limited environment without worrying about doing something adverse to the larger production network.
- (b) These Pilot Networks can be interconnected with each other to know how they will communicate and what problems are likely to be faced in interoperability.
- (c) With the aid of the Pilot Network, enough information can be gathered that can be used to identify potential pitfalls that may occur and identify hardware and software purchases that may be needed.

3.7.1.3 Perform a comprehensive compliance and security audit

- (a) After having the hands-on experience in IPv6, each organization must then understand their existing network infrastructure. An audit allows the organization to know in details if there are any problems with the infrastructure and if all of the organizations

existing hardware and software supports IPv6. There are 2 main audits that have to be performed which are the IPv6 compliance audit and security audit.

- (b) Organizations are advised to appoint auditors to perform compliance and security audit. Generally the service providers and equipment vendors having experience in IPv6 can perform this function.
- (c) An IPv6 compliance audit will help an organizations to decide the following:
 - a. Identify any changes that may be needed to their network infrastructure.
 - b. Identify hardware used and the level of support of IPv6.
 - c. Review existing network diagram to better plan IPv6 deployment.
- (d) From the outcome of the audit, organizations can make a conscious decision on IPv6 deployment and the type of traffic that will pass through. The following questions have to be taken into consideration seriously:
 - i) Is the packet handling done at the hardware level or software level? - Some hardware may allow a firmware upgrade that allows processing of IPv6 packets. This usually means that the packet is handled at the software level. If the packet handling is done at the software level, the amount of processing will increase and the number of packets processed will drop.
 - ii) What are the routing schemes used and their support of IPv6? Will both internal and external routing protocols be used? - The routing protocols such as RIP, OSPF and BGP have their own versions for IPv6 and are not backward compatible with IPv4 which means there will be **TWO** different routing traffic on the network (IPv4 and IPv6).
 - iii) Do the Layer 3 switches (VLAN) and load balancers have support for IPv6 and what changes have to be made? - Organizations already have these devices in place therefore in order to provide complete IPv6 functionality; these devices have to support IPv6. Upgrading these devices should be done with care and consideration as any mistake would affect global Internet connectivity for both IPv4 and IPv6.
- (e) The security audit will help to identify areas that are lacking in security implementation and how it can be improved. It is not desirable to introduce a new technology without first being sure the existing infrastructure is as secure as possible.
- (f) The security audit will consist of 2 areas that are:

- i. The external audit covers the following: (Development of external audit criteria)
 1. Site scans
 2. Remote audits
 3. Penetration tests
 4. Spoofing of IP or email

- ii. An internal audit covers the following: (Development of internal audit criteria)
 1. Evaluating existing network diagram
 2. Interviewing of administrators for:
 - a. Physical access and infrastructure audit
 - b. Security devices
 - c. Routers
 - d. Operating Systems
 - e. Applications such as SSH, Telnet, databases, internal business applications.
 3. Site scans
 4. Penetration tests

(g) The outcome of the audit will be used to strengthen the existing infrastructure and help to determine whether:

- i. Are best practices implemented in the current infrastructure?
- ii. Are there any unwanted or unknown IPv6 traffic on the infrastructure?
- iii. Is the firewall able to detect and block 6to4, ISATAP tunnels (Protocol 41) and IPSEC tunnels (Protocol 50 - ESP and 51 – AH).
- iv. IPv6 security considerations as in Appendix-C can be referred in the process of implementing IPv6.

3.7.1.4 Set up applications to take advantages of IPv6

- (a) Below are some of the example applications that can make use the features of IPv6.
- a. Internal messaging system for organization's use via IPv6.
 - b. Internal organization's website that is accessible via IPv6.
 - c. Mail server for internal use via IPv6.

- (b) At this stage, it is advised not to change any crucial applications as doing so might cause problems throughout the organization . Each organization must be aware of this during the audit and planning stage which will give the organizations the knowledge to overcome any issues. Any attempt to migrate the crucial applications will only be done in Phase 3.

3.7.1.5 Evaluation of implementation

- (a) An evaluation has to be conducted after the implementation within the organization. This helps us determine if everything meets our requirements. It should cover the following at the very least:
 - i. Is the timeline stipulated at the start of the project met?
 - ii. What were the pitfalls and issues faced during transition?
 - iii. Which areas require more focus and attention?
 - iv. Has the implementation got the organization closer to its business needs?
 - v. Is the organization ready to perform the transition to other areas or branches?

- (b) After the review, the organization can begin to determine what additional tasks it has to perform to make other deployments easier.

3.7.2 Phase 2

The objective of Phase 2 is to replicate the Phase 1 setup in a Regional/ branch offices. This allows the organizations to have a secondary location to test enhanced features of IPv6.

Listed below are the tasks that have to be done at the other Regional/branch offices of the organizations:

- (a) Plan the budget, network architecture and other considerations.
- (b) Set up a Pilot network.
- (c) Perform a comprehensive compliance and security audit.
- (d) Set up applications to take advantage of IPv6.
- (e) Evaluate the implementation.

The same considerations done in Phase 1 for the above tasks applies.

3.7.3 Phase 3

Phase 3 is geared towards transition of the primary applications to maximize the use of IPv6 features which would improve performance, stability and security. It is best to choose an application that has a significant value to the organization for the transition process.

3.8 Other Important Aspects to be considered by the Organizations

3.8.1 Some features of IPv6 that can provide benefits and enhancements to applications

(a) End-to-end

- i. Application deployment and development becomes easier as the developer does not develop logic for dealing with intermediate systems such as NATs.(NATs compromise end-to-end security as it modifies packet headers similar to what an attacker would do for spoofing).

(b) Security

IPSec is mandated to be deployed as part of IPv6 deployment, therefore end-to-end security is now possible, which avoids packet sniffing and obtain sensitive information.

(c) Quality of Service (QoS)

Applications can be given priority depending on their type for example real-time applications such as VoIP will be processed first before other traffic such as HTTP. This improves the quality of the transmission for certain applications and services.

(d) Multicast

Provides better bandwidth utilization for example it offers an efficient backup strategy to various off sites to ensure data redundancy

(e) **Anycast**

- i. Offers decentralization to provide a user of the application to access the server closest to their location.
- ii. Alternative way of doing load balancing and redundancy as the servers can be scattered throughout different parts of the organization or world thus reducing a single point of failure. Using this technique, users can be directed to the location where the data they are seeking is stored instead of obtaining it only from a single source.

3.8.2 Some considerations for application development

- (a) Ensure full understanding of impacts and gains for every feature above and how it can best be leveraged to provide the maximum return.
- (b) Work closely with the application provider in order to understand their roadmap and plans for the application.
- (c) At times, it is more cost effective in the long run to change an application to take advantage of the complete IPv6 feature set though in the short run there would be extra cost and training period for end users.

3.8.3 Making the existing application IPv6 aware

- (a) Before proceeding to utilize all the new and great features of IPv6, it would be better to make the current application to be IPv6 aware. This process would help us identify problem areas. Potential issues to look for are:
 - i. The application was purchased and the vendor is no longer supporting it.
 - ii. It's an in-house built application whereby the current developers are not trained in developing applications for IPv6.
 - iii. Modifying or migrating the current application would incur a high cost in data transition.

The above list is not exhaustive and there are other issues that may occur. Application transition requires the organization to work closely with the application provider during this Phase. If the application does not support the features, it would be better to assess other systems that may offer similar functionalities. However this is dependent on the application

and needs of the organization. Performing a comparative analysis on two identical applications with all the benefits enabled would help identify the returns and benefits of performing a complete overhaul of the application.

3.8.4 Some options for application transition

(a) Off the shelf application

- i. Inquire from the vendor if the application being used has a newer version that supports IPv6 and also what changes need to be made i.e. patching of application only or transition to an entire new version.
- ii. Obtain a demo copy and test in the network to ensure that the application works as intended with or without the added features of IPv6.
- iii. If data transition is needed, discuss with the vendor on how the existing data can be migrated to the newer version and whether they will provide assistance or tools available that can perform the transition.

(b) Customized application

- i. Contact the developers and inquire what steps can be taken to migrate the application.
- ii. The steps from (a) can be applied to ensure a smooth transition.

(c) In-house application

- i. Ensure the in-house developers are trained in developing IPv6 applications and if they are insufficiently trained, require them to attend the necessary training.
- ii. The training should at the very least cover the following:
 - a. Writing portable applications to work on various operating systems.
 - b. Be security conscious when writing applications.
 - c. Writing protocol independent programs.
 - d. Finding portions to rewrite and reorganize code.

- iii. Training is not tailored to a specific programming language. Once the developer is exposed to the concepts, it should be sufficient for them to know what needs to be done. However, if training in a specific language is required, they will need to attend it in addition to the above training.

(d) Open source application

- i. Check if the application supports IPv6.
- ii. Contact the project owner and inquire how the organization can provide assistance in helping the transition of the application.

Once the application has been made to support IPv6, begin testing it in a controlled environment (Pilot Project from Phase 1 could be used for this purpose) thoroughly for any issues and do the necessary to get it working as required. It will be necessary to work closely with the provider of the application in hunting down bugs and issues that might occur. The deployment of the application would also depend on the infrastructure and architecture as there are two sets of access policies (IPv4 and IPv6) that have to be considered.

After the application passes the rigorous testing, deploy the application throughout the entire organization. Ensure adequate information is available to assist the tech support personnel in aiding users that might encounter problems.

3.9 Modified Approach due to Time Constraints

The IPv4 exhaustion date is approaching fast and the organizations have only 2 years to implement IPv6 in their organizations. In normal circumstances, all the three phases proposed above could have been done one after the other by the government departments. However, this would cause the implementation to go beyond the exhaustion date. Therefore, govt. departments will have to implement all the 3 phases together.

3.10 Recommended Approach for India

- i. All ministries and Departments of the Central and State Governments must Inventory their network infrastructure. It should be clearly listed out what equipment is ready for IPv6 and what is not?

- ii. IPv6 ready equipments in the procurement requirements as a MUST. The Department of Telecommunications has already issued instructions to all Central and State governments in this regard.
- iii. Various government departments can prepare their transition plan to IPv6 with the assistance of their service providers.
- iv. Create an IPv6 transition team in each ministry in close coordination with Dot/ TEC level
- v. Set up pilot networks in non-core segments in each department / ministry to gain the experience of deploying IPv6. These pilot networks can be connected to each other for doing interoperability testing. Once the experience is gained, the pilot networks can be scaled up to cover all the segments of the department /Ministry.
- vi. Transition can start by introducing the first application using IPv6 for the web sites of the government

3.11 Time Plan for Migration

The Government Departments can follow the modified time table given below for completing the various activities related to transition to ensure that transition is completed before March-2012.

The approach proposed here is similar to the one recommended for the service providers. All Government Organizations shall complete the transition process by March-2012. **In this process the designated working group in the Task Force shall coordinate with the nodal officers in different government departments to complete the transition process.**

3.12 Actionable points

1. Creation of one IPv6 working group in each ministry/department.
2. Adhering to the generalized transition plan given in this document. The actual details can be worked out separately by each ministry / department in coordination with the concerned working group of the Task Force.

-----x-----

	4
--	----------

<p>Action Plan for Service Providers</p>

4.0 Introduction

This chapter presents a series of recommended action plans and milestones to prepare towards the IPv4 exhaustion, which is expected to occur in mid-2012. The plan attempts to provide a reference to industry players. It is expected that the industry players will study and address the issues in IPv4 address exhaustion on the basis of this reference, and create and execute individual action plans accordingly. It is hoped that the Internet industry as a whole will smoothly overcome this problem as a result by adequately preparing themselves by being ready with IPv6.

The roadmap is an estimate and presents the worst case scenario for an organization which has still not started its journey towards IPv6. The actual dates will depend upon how fast or slow different stakeholders are ready to implement IPv6 in their organizations. Some critical dates are as below-

- 1) Various study reports have predicted the exhaustion of IPv4 addresses by mid-2012. Around mid 2011 to early 2012, exhaustion of the international address blocks (IANA pool) will happen.
- 2) Acquiring new IPv4 addresses by India after mid-2012 would become extremely difficult, if not impossible. This will put severe stress on services which demand IPv4 e.g. wireless internet, broadband etc. It is estimated that APNIC will exhaust IPv4 between 2Q-3Q of 2012.
- 3) It is expected that as the exhaustion date will be closer factors such as last minute demand may cause exhaustion earlier than expected.

4.1 Discussions with Service Providers on Transition Plan

During the year 2009-10, TEC has conducted a number of national IPv6 workshops in association with CMAI and the IPv6 forum with different service providers and other stakeholders at Delhi, Bangalore, Chennai, Mumbai and Kolkata. In addition one International Summit on IPv6 was also conducted in Delhi. Further one exclusive meeting was conducted in TEC, New Delhi with different service providers, industry associations to discuss their transition plans. Based upon the interactions in these workshops, many service providers submitted their transition plans. Some organizations also responded by saying that they have no plans.. Based upon the plans received from different organizations, it is found

that large service providers are generally on track but efforts have to be made by the smaller service providers to get ready in time. The summary of transition plans of different service providers is given below –

4.1.1 TATA Communications

Tata communication is able to offer IPv6 internet connectivity to its customers today. Tata communication limited is the upstream service provider for the Tata communication internet services limited (TCISL)

S.no	Action	Target date
1	All DNS servers are IP ready.IPv6 forward DNS services has already been implemented & tested on infra domain name	Completed
2	IPv6 connectivity for enterprise costumer	Completed
3	Testing for IPv6 connectivity for TCISL customers	Under progress
4	All the servers & load balancer to be procured would be IPv6 complied and ready for service.	June 2010
5	Procurement of new hardware	July 2010
6	TCL all routers are IPv6 compliant, TCISL will complete procurement of new hardware	July 2010
7	Installation of new hardware	Sept 2010
8	Testing of new hardware	Nov 2010
9	TCL had conducted pilot test, pilot project for TCISL	Nov 2010
10	IPv6 connectivity for retail broadband costumer	Dec 2010

4.1.2 Bharti Airtel

S.no	Action	Target date
1	IPv6 Pool Allocation from APNIC	Completed
2	Mandatory IPv6 Feature support for procurement of new equipment	FY 09-10
3	IPv6 Network Address Planning for IP backbone	Completed
4	IPv6 based Peering with International Carriers	Completed
5	Testing / Demo Facility for testing IPv6 based services	Established
6	End to End Testing of IPv6 based VPN services	In Progress
7	IPv6 support assessment for network, services and support infrastructure	Q2 FY 10-11
8	IPv6 support on existing routers by software upgrade	In Progress
9	Sample Live IPv6 Customer	Commissioned
10	IPv6 based DNS deployment (One Server)	Commissioned

4.1.3 Reliance Communications

They have mentioned that IPv6 peering with NIXI is completed in Delhi and Mumbai. They are adopting the 6PE approach for transition. However, no specific timeframes have been given.

4.1.4 MTNL

Sr.No.	Activity	Target date
1.	Procurement of equipments, networks, devices with IPv6 capabilities	Immediately
2.	(i) Allocation of IPv6 address block from APNIC (ii) Preparing inventory of IPv6 capable and not capable equipments (iii) Migration of gateways and NiXI connectivity	Dec-2010

3.	Migration of ISP setup	Dec-2011
4.	Migration of access networks / customer equipments	As and when needed according to procurement cycle and life cycle of equipments

4.1.5 IPv6 Deployments in Sify

- Sify is the pioneer in testing and deployment of IPv6 technologies and its associated services in India.
- Sify has a dual-stack (IPv4 & IPv6) compliant edge with an MPLS enabled NGN core supporting transport of IPv6 packets alongside IPv4
- With the dual-stack edge, Sify can offer IPv6 VPN & Internet transit services to its enterprise customers.
- Sify is part of 6Bone an IPv6 IXP. All its assigned IPv6 numbers are advertised to the public Internet through 6Bone
- Sify has deployed <http://sify.com> as the first dual-stack commercial content portal in India.
- Sify is the only private ISP member in the project 6Choice, a India – Europe cooperation for promoting IPv6 adoption. Sify is funded for developing case-studies based on its experiments to promote IPv6 migration in the Industry.

4.1.6 Hathway Cable and Datacom Limited

Sr.No.	Activity	Target date
1.	Procurement of equipments, networks, devices with IPv6 capabilities	Immediately
2.	Core Infrastructure IPv6 compliant	Done
3.	Transition of Data Centre to IPv6	Started
4.	Provisioning System	June-2010
5.	CPE equipments(~ 95%)	Done
6.	IPv6 address block allotment from APNIC	Done

4.1.7 Ortel Communications Ltd.

S.no	Action	Target date
1	Phase 1 1. DOCSIS 3.0 CMTS in Mar 2010 2. Get IPv6 Address from APNIC 3. Procure Dual Stack Core Router 4. Procure DOCSIS 3.0 Modems 5. Procure IP Commander with DHCP,TFTP & DNS with both IPv4/IPv6	Mar 2010
2	Phase 2 1. Upgrade existing CISCO router to Dual Stack Op 2. Upgrade firmware of DOCSIS 2.0 Modem to IPv6 3. Procure more DOCSIS 3.0 Modem.	Jul 2010
3	Phase 3	Oct 2010
4	Phase 4	Dec 2010

4.1.8 Dishnet Wireless Ltd.

S.no	Action	Target date
1	IPv6 Allocation from APNIC Done	Done
2	IPv6 Peering with NIXI Done	Done
3	Planning for Procurement of Equipments 1-Feb-10	Completed
4	Identification of Router and IOS 25-Feb-10	Completed
5	Testing of IPv6 Service on test bed 30-Apr-10	30-Apr-10
6	IPv6 DNS Implementation 20-May-10	20-May-10
7	Hosting of IPv6 server 15-Jun-10	15-Jun-10
8	Procurement of Equipments by 14-Aug-10	14-Aug-10
9	IPv6 Peering with global service provider 30-Sep-10	30-Sep-10
10	Introduction of IPv6 Device 30-Sep-10	30-Sep-10
11	IPv6 IPs Allocation Policy 30-Oct-10	30-Oct-10
12	IPv6 Service Offering 10-Nov-10	10-Nov-10
13	Testing Phase for IPv6 30-Nov-10	30-Nov-10
14	Launch of IPv6 Service 15-Dec-10	15-Dec-10

4.1.9 HCL Infinet Ltd

S.no	Action	Target date
1	Phase-1 Implementing IPv6 in core	15 July 2010
2	Phase-2 Implementing IPv6 in internal network and services	30 July 2010
3	Phase-3 Implementing IPv6 at our customers end	31 Oct 2010

4.1.10 Beam Telecom Pvt Ltd

- (1) It is a continuous process to ensure that all the core, edge and access equipment is compatible for IPv6 adoption for the last two years.
- (2) Adoption of IPv6 at appropriate time as business demands. However, a well drafted transition plan is in place that is being reviewed continuously. Whenever they assign IPv6 networks, they update required "whois" records for the benefit of the community.
- (3) The adoption process will begin with migrating "Management network", that is used for remote managing all the active devices on the network to IPv6.
- (4) Once the management network is stabilized, they will begin assigning IP addresses to some of the customers requesting IP address using DHCPv6 Discover packet.
- (5) In parallel, they will also migrate their in-house network to IPv6 allowing users to get acquainted with the same.
- (6) At a later stage, they will migrate their Enterprise and Hosted customers to IPv6 when asked for.
- (7) During the above process, organization will be implementing required network elements to support the transition.
- (8) While the organization understands that there need not be any set defined target dates for such migration, they will be working towards aligning their network with such similar networks in the region.

4.1.11 West Bengal Electronics Industry Development Corporation Limited.(WEBEL)

WEBEL is a Category-B ISP connected to "Category-A" ISPs. Depending on customer's requirement and getting the IPv6 IPs from these "Category-A" ISPs Webel ISP can implement IPv6 addresses as the core device is compatible to IPv6. However, these

category – A ISPs need to implement IPv6 at their end first and guide Webel ISP accordingly before any migration plan or pilot project.

4.1.12 Tulip Telecom Ltd

S.no	Action	Target date
1	Phase 1 : Enabling Edge for ipv6 .Making dns test ready.	2 months
2	Phase 2 : Enabling Core for Ipv6 (including testing).	6-8 months
3	Phase 3 : Enabling access .	after completion of the above .

Stage 1 – Creation of IPv6 islands of access networks. This stage involves creation of IPv6 islands and connections of them to IPv6 internet through IPv4 network

Stage 2 - This stage consists of converting the core IP network to dual stack supporting IPv6 and IPv4.

Stage 3 - This stage consists of converting the core IP network to IPv6 with IPv6 edge and a few dual stack edges

Stage 4 - The few dual stack edges of stage-3 after the end of life shall be replaced by IPv6 edges leading to IPv6 only situations

4.1.13 CJM Consultancy Services Ltd

S.no	Action	Target date
1	Procure dual stack core router	April 2010
2	Procurement of IPv6 compliant equipment	As per requirement

4.1.14 Singtel

Singtel is fully IPv6 enabled and their hardware is fully IPv6 compliant

4.1.15 Equant Network Services India Pvt.Ltd

IPv6 is supported on the existing network infrastructure since May 2009. All new deployment of access layer devices will be IPv6 compliant. Existing access layer platforms (PE router) that do not support IPv6 have been replaced by IPv6 compliant platforms (Cisco 7600 and ESR 10K). Customer premises equipments (Equant managed) and access layer devices will be Dual stack enabled.

4.1.16 AT &T Global Network

S.no	Action	Target date
1	Large scale migrations are not required or anticipated	
2	currently conducting controlled introduction of IPv6 based transport and MPLS VPN which will continue	Throughout 2010&1 st half of 2011.

4.1.17 Netmagic solutions

Production setup will be on dual stack environment, below are the layer wise description

Core - Existing MLX/XMR supports ipv6

Aggregation - Aggregation layer devices do not support ipv6. Evaluating Cisco, Foundry and Extreme switches which supports ipv6.

Access - Access layer devices does not support ipv6. Evaluating cisco , force10,foundry and HP for IPv6.

Others -

- Continue implementing IPv6 in the IP-core, move to native IPv6 transport when possible.
- Ensure that increase in IPv6 load can be handled, long-term plan.
- Continue implementing IPv6 further out in the network (closer to the end customer).
- Prepare for native IPv6 access for IDC customers.
- Help for migration of customers hosted within our IDC.
- Replace existing network devices with ipv6 capable devices.
- Configure device for dual stack with existing ipv4 addresses, then introduce IPv6.

4.2 Time Plan for Transition

Considering the worst case scenarios, the milestones in the following roadmaps have been given, which service providers can follow. Some organizations may be in a better situation whereas some may be in a worse situation. However, whatever be the case, all

service providers shall target to handle IPv6 traffic and offer IPv6 services by December-2011.

4.3 Action Plan for the ISPs

1. Policy Development, Decision making by Management
 - i. Analyze the impact of exhaustion on the organization
 - ii. Perform the business decision for the preparation policy
 - a. Whether to ignore the exhaustion issue? How to solve the problem? (use IPv6?). when to solve the problem? Which type of access network is needed?
2. Business Planning, Review, service Planning
 - i. Policy detailing and the business plan development – It includes service planning, basic network design, consideration of operating procedures and systems etc.
3. Design, Technology, verification – The design and technology of the equipment being purchased has to be confirmed and verified for IPv6 functionality
4. Equipment selection, procurement, system building – Actual selection, procurement and installation of the IPv6 equipments
5. Preparation of O&M system – Preparing the Operation and Maintenance systems
6. Workforce Training – Training the workforce well in advance to install, operate and maintain the systems
7. Launch basic services – Launching of services for customers

Table 3: ACTION PLAN FOR NETWORK PLAYERS (ISPs)

	2010	2010	2010	2010	2010	2010	2010	2010	2010	2010	2011	2011	2011	2011	2011	2011	2011	2012	2012	2012	2012	2012	
	1-2-3	4-5	6-7	8-9	10-11	12-1	2-3	4-5	6-7	8-9	10-11	12-1	2-3	4-5	6-7	8-9							
Policy Development																							
Decision making by management																							
Business Plan Making, Service Planning																							
Business Plan Decision																							
Design, Technology Verification																							
Equipment Selection																							
Equipment Procurement, System building																							
O&M System preparation																							
Workforce Training																							
Launch Basic Services																							

4.4 Action Plan of ASP/CSP

It involves the following steps –

1. Policy drafting, Management decisions making
2. Technology verification, system building
 - a. Platform verification, selection and building
 - i. Server, OS, middleware
 - b. Service infrastructure design, verification and building
 - i. DNS, Load balancer, firewall etc.
3. Application, content
 - a. Verify applications and contents under exhaustion situations (i.e. when IPv4 is no longer available and only IPv6 is available)
4. O&M system
 - a. Verify the correct behavior of the system log, database, operation system under the exhaustion situation
5. Workforce training
6. Launching the basic services

4.5 Actionable points

1. To start with major Service providers (having at least 10,000 internet customers or 1-STM bandwidth) will have to adhere to the general transition plan proposed here and they shall target that their networks are ready to handle IPv6 traffic and offer IPv6 services by December-2011. This will be followed by smaller ISPs who need expertise and guidance for transition, which can be provided by the Network Implementation Working Group in the Task Force. All smaller ISPs shall make efforts to provide IPv6 services before exhaustion of IPv4 addresses.

-----X-----

	5
India IPv6 Task Force	

**India IPv6
Task Force**

5.0 Introduction

The transition from IPv4 to IPv6 will affect many organizations. At the same time it is not possible for any one organization to bring about this change. It has to be a coordinated national effort among different stakeholders. During the various workshops conducted by TEC throughout the country, it has emerged to create a task force for deployment of IPv6 in India. This is the method adopted by many countries around the world for facilitating the deployment of IPv6 in their countries. The Task Force will bring together all the different stakeholders to a common platform where they can together discuss the issues, develop and implement the strategies for making the transition to IPv6 possible.

The goal of the Task Force will be to examine the impact of IPv4 address exhaustion from the varying standpoints of the different players involved in the provision of network systems (infrastructure providers, equipment vendors, system integrators, service providers, etc.), imparting the need for an industry-wide recognition of issues and consideration of strategies and countermeasures. The Task Force will emphasize and facilitate the importance of the open sharing of information. As a collaboration of Telecommunications and Internet-related Associations, the Task Force will integrate the resources of various member communities, actively working towards the smooth continuity of Internet-based business throughout the process of and following the exhaustion of IPv4 addresses.

The Creation, structure and working of the Task Force is one of the approved actionable points emerged during five different National IPv6 awareness workshops, one International Summit in Delhi and one exclusive workshop with the service providers, nodal officers and industry associations held by TEC during FY2009-10. The structure is based on the feedback received in these workshops and the summit.

5.1 Duration of Existence of the Task Force

It is once again highlighted that approximately 2 years time frame is available before new IPv4 addresses are more or less depleted. After 2 years our networks can continue to grow only if they adopt IPv6. Even after that the transition of existing IPv4 networks to IPv6 will continue. Transition of all communications networks from IPv4 to IPv6 is a long term

process. It will take many years for IPv6 to replace IPv4 and establish itself. It will not happen overnight. Therefore, there is a need to have a permanent establishment to deal with all IPv6 related issues in the years to come. This type of establishment has already been set up in some countries but presently India has no such establishment. When this institution is set up in, it can be named “Indian IPv6 Centre for Innovation”.

The Task Force is only an intermediate short term solution to take up all the IPv6 related issues on priority. ***In the long term all activities of the Task Force will be taken over by the “Indian IPv6 Center for Innovation” once it is established.*** The Task Force can be wound up after the ***Indian IPv6 Center for Innovation*** has acquired enough capabilities to carry on the unfinished work of the Task Force in the future.

5.2 Action Items for the Task Force

The task Force will take up activities in the following key areas.

- 1. Raise awareness on the exhaustion of IPv4 and impact of IPv6 on proliferation of Internet and broadband in the country**
 - Activities related to enlightenment, publicity and education
 - Organizing training programmes, workshops, conferences and tutorials
 - Advice to the Government on Policy issues dealing with IPv6

- 2. Encourage all stakeholders to begin the initial phases of IPv6 readiness**
 - To synchronize the activities of various stakeholders
 - List up the issues to solve by each player
 - Information sharing among member organizations
 - Advise to member organizations on IPv6 technical issues during the transition process
 - Identification of challenges and solutions using IPv6
 - Outreach to new stakeholders suffering from IPv4 address exhaustion

- 3. Development of transition plans in subsequent phases to support a smooth and wide transition to IPv6**
 - Conduct surveys, studies and review of the progress by different organizations and the country as a whole during the transition process

4. Undertake series of impact assessments / business cases

- Coordination with different agencies for the purpose of IPv6 standardization
- Create pilot projects for IPv6 capability demonstration
- Increase R&D coordination between academia and industry

5. International cooperation in IPv6 related areas

- Increasing coordination with international organizations, neighboring and other countries for IPv6 deployment
- International collaboration with other similar Task Force organizations in the world

Structure of “India IPv6 Task Force”

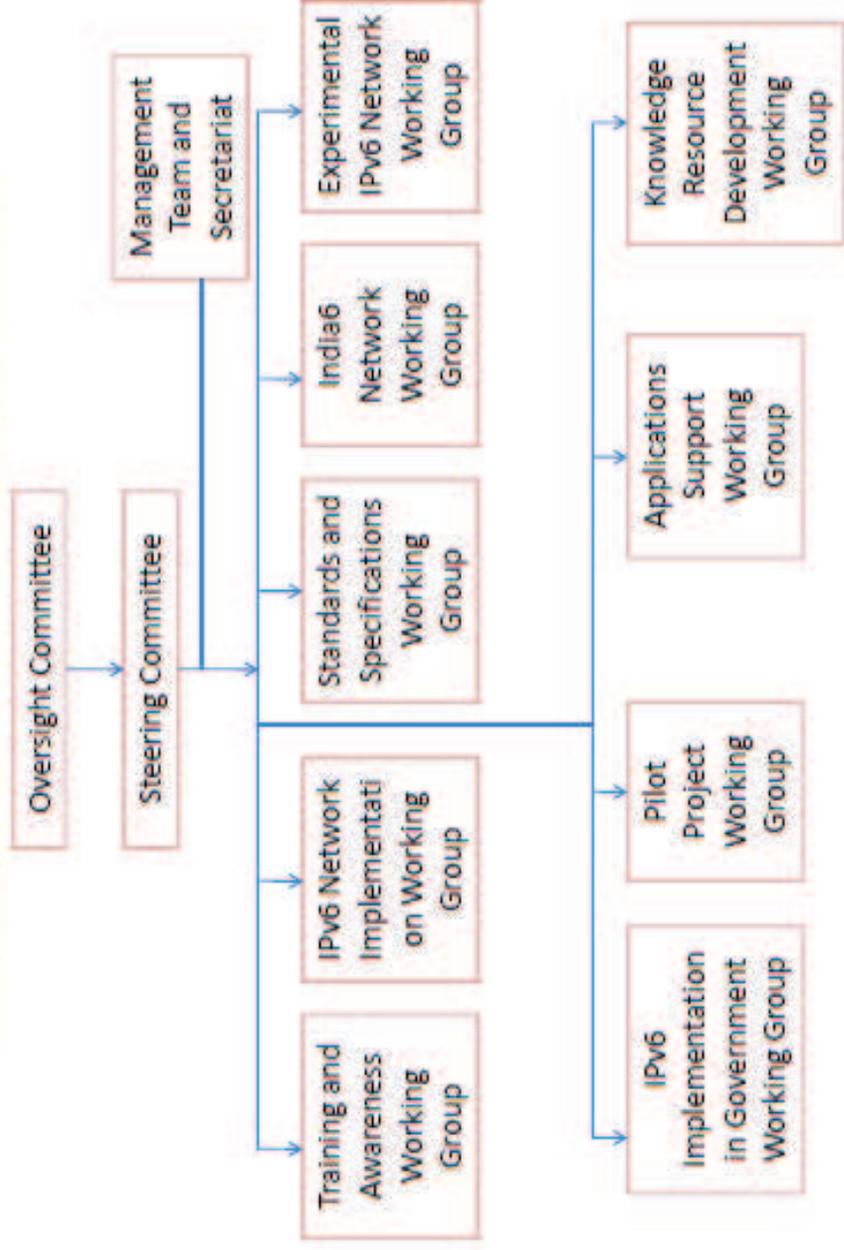
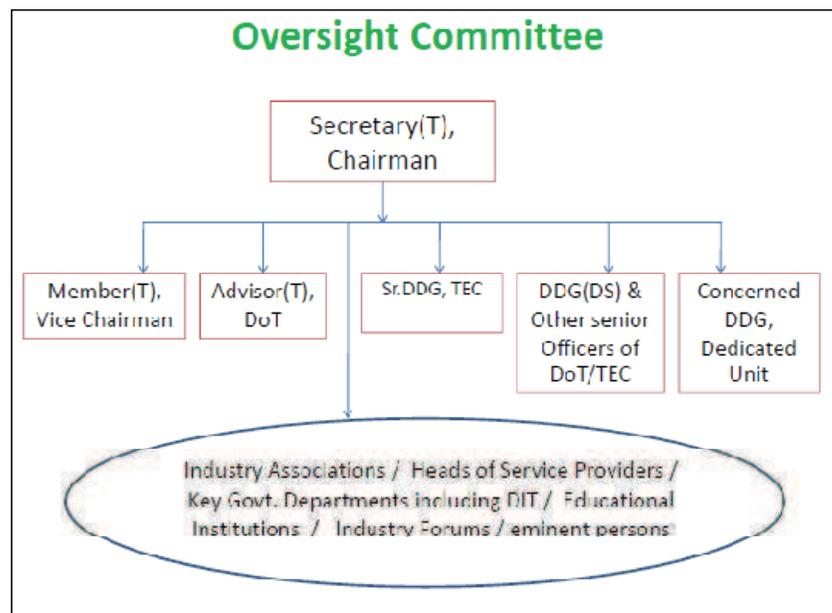


Figure 8: Structure of India IPv6 Task Force

5.3 Structure of Task Force

1. **Oversight Committee** – This will be the apex body for making policy decisions and responsible for guiding the task force by taking strategic decisions. Its role will be to provide the strategic national directions for the movement of IPv6 in India. It includes providing the vision, mission and strategic plan for IPv6 implementation in India.

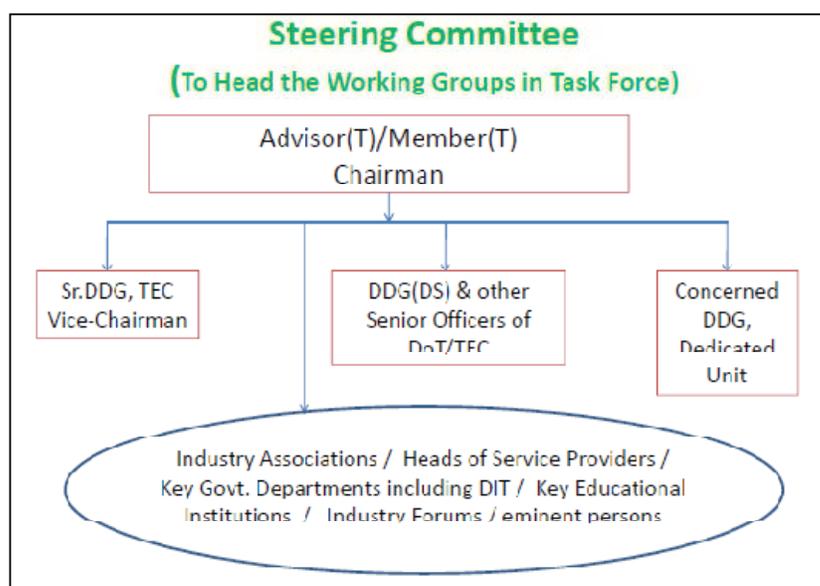
Figure 9: Composition of the Oversight Committee



The members of the Oversight Committee will consist of heads of service providers in the country, who will take up different activities in the working groups. It will also have members from key government departments, Industry associations, educational institutions and different industry forums and persons of eminence. The Oversight Committee will be headed by Secretary(T), DoT as its Chairman, Member(T),DoT as its Vice-Chairman ,Advisor(T) DoT, Sr.DDG, TEC and other senior officers of DoT as members and concerned DDG of Dedicated Unit as the member convener. The Oversight Committee will normally meet every 4 months. The membership of the Oversight Committee shall be limited to 20, however Chairman can nominate additional members as and when required.

2. **Steering Committee** – The Steering committee will be the second level body for coordinating the activities of the Task Force. It would perform the following important functions –
- a. To oversee the activities of the different working groups constituted under the Task Force for timely smooth transition in the country.
 - b. To coordinate with different Central, State Government Departments and all other stakeholders including service providers for taking full advantage of IPv6 applications in the country.

Figure 10: Composition of Steering Committee



- a) The Steering Committee will be headed by Advisor(T)/Member(T), DoT as Chairman and Sr.DDG(TEC) as Vice-Chairman and the concerned DDG, Dedicated Unit as Convener. In the absence of Advisor(T), Member(T) shall function as Chairman of the Steering Committee. The Steering Committee will also have senior officers and office bearers from various other stakeholders as members. Additional members can be nominated by the Chairman of the Steering Committee. The Steering Committee will normally meet every 2 months.
- b) To coordinate with the activities of different working groups, the Steering Committee will have the heads of the various working

groups as members. Alternatively, it can have members from the lead organizations of these working groups. Additional members can be inducted depending upon the type of activities performed by different working groups.

- c) There are more than 100 different central and state government ministries, departments and PSUs. The DoT has already issued instructions to them for appointment of nodal officers for facilitating the transition from IPv4 to IPv6 in their respective organizations. To coordinate with these nodal officers from the different central and state governments and other related work it is proposed to entrust this work to a dedicated unit with one DDG and three Directors level officer in DoT.
- d) In addition, the steering committee will also have the nodal officers of important ministries/departments as members. To begin with we may have as members the nodal officers from Department of Information Technology, Department of Science and Technology, Ministry of Defence, Ministry of Railways, Ministry of Power and Ministry of HRD, Ministry of Home Affairs, Ministry of Information and Broadcasting. Nodal officers from other ministries or departments can also become additional members depending upon the quantum of transition work involved and the concerned DDG of Dedicated Unit shall take decision in this regard.
- e) The Steering Committee will also have members from other stakeholders like the IPv6 Forum, IPTV Forum, IPv6 equipment manufacturers and vendors etc. In addition to above, the Steering Committee would also have adequate number of JAG level officers from DoT/TEC as members for coordination in all technical matters pertaining to transition.
- f) A three members subcommittee headed by the Convener of the Steering committee will approve the members of the different working groups and will sort out their routine problems. The other 2 members shall be concerned DDG/Director from TEC/DoT and shall be nominated by chairman of the steering committee.

3. Deployment Working Groups – Under the Steering Committee, there will be different working groups. Each Working group will be responsible for specific activities associated with transition to IPv6. One of the member organizations of each working group will become the lead organization in that working group. The lead organization will be responsible for funding the activities of the respective working group in addition to other activities like place of meetings, logistics, selection of members etc. The distribution of activities amongst different stakeholders is given separately. The members of each working group shall meet at least once every month to review the progress of that working group.

5.4 Member Organizations

The members of the Task Force will broadly belong to the Government, Industry and Academia. The members in the Task Force shall be mainly from the following organizations/stakeholders in addition to others.

- DoT/TEC/CDoT
- DIT (NIXI, ERNET, NIC etc.)
- Different central/state Government Departments
- All telecom and internet service providers
- Educational Institutions (IIT, IISc, Etc.)
- Industry Associations
- IPv6 Forum, India
- Equipment Vendors
- Content Providers

- Software vendor
- Cable TV Industry representatives
- Persons of eminence

5.5 Working Groups

Each working group will consist of members drawn from different organizations who are members of the Task force. The members should be so selected that adequate representation is given to all service providers / stakeholders. One organization will become a lead-member in each working group for guiding and funding the activities of that working group. The different types of working groups are given below -

1. **Training and Awareness Working Group** – The training requirement for having an adequate pool of IPv6 trained manpower in both the government and the private sector is huge. E.g. For the government sector alone, there are about 100 different central government departments / ministries. Each department/ministry has about at least 100 different units including PSUs and their wings etc. There are 34 states/UTs and each one has about 100 different state government ministries, departments and PSUs . By conservative estimates, even if 5 persons are required at each place the demand is a staggering 67,000 persons(Approx.) to be trained on IPv6, just for the government sector alone. Even these are very conservative estimates. The demand by the private sector will be separate. Therefore, the potential for training and awareness is huge.

There are various types of activities like –

- a. Hands-on trainings in association with APNIC, IISc and other organizations
- b. IPv6 Certification programmes for qualified engineers
- c. Network engineers trainings
- d. Trainings for nodal officers from government
- e. Conducting Workshops, seminars and conferences

This working group will be responsible for conducting the above activities for benefit of all stakeholders. This WG will follow the “Train the Trainer” concept. It will be responsible for developing the trained manpower required by different organizations in the government and the private sector to deal with the different

types of IPv6 transition issues. The Working group can also explore revenue generation through the above activities.

2. **Action Plan and IPv6 Network implementation working Group** – This working group will be primarily responsible for studying the different network scenarios and come up with action plans for individual service providers / organizations. Different organizations are likely to have different network scenarios, so they will have unique needs in their organization. This group will assist them to create a tailor made action plan for them for transition to IPv6. This working group can also have “on-demand project” teams which can give on-site support or specialized assistance to organizations who need help for IPv6 deployment. TEC will be an active member of this working group as all the nodal officers appointed by different organizations for deployment of IPv6 would be interacting with TEC.
3. **Standards and Specifications Working Group** – This working group will coordinate with TEC for development of common IPv6 specifications for the country, which will be followed by all stakeholders. This working group will also coordinate with the IPv6 Ready Logo committee of the Ipv6 Forum to plan and advise different stakeholders and organizations like vendors, ISPs, Websites etc. for obtaining the IPv6 Ready Logo. This working group will also interact with other standardization bodies around the world like USGv6, NIST USA, JATE Japan, Nav6 Malaysia, etc to participate in various standards and specification development processes.
4. **“India6” Network Working Group** –
 - a. **Concept of Transition Pipe** – Most parts of the Internet are based on the IPv4 protocol. As the transition to IPv6 will happen gradually, during the transition period, islands of IPv6 networks will come up in different organizations spread far and wide. The problem is that organizations hesitate to migrate to IPv6 because they are not sure whether they will be able to send IPv6 traffic to another IPv6 network because of the absence of any nationwide “**IPv6 carrier network**” in between.
 - b. **Need for a “Transition Pipe”** - This point has been often raised by service providers/associations in various workshops and meetings. They want a

“Transition Pipe” for carrying IPv6 traffic from one IPv6 network to another IPv6 network. At present there is no such pipe at all-India level so IPv6 traffic remains isolated in closed networks. The absence of such a “transition pipe” is hampering the growth of IPv6 in India. There exist similar networks in all the countries, which are at the forefront of the IPv6 revolution, e.g. CNGI (China Next Generation Internet). In India also this type of network can be built and can be named as “**India6 network**”. *In fact service providers have suggested that the Government should take initiative in this area and build this “Transition Pipe”. Another perceived benefit of having the IPv6 “Transition Pipe” in place is that it would facilitate the penetration of broadband in our country, since future development of broadband in India will depend on IPv6 only.*

- c. **Prerequisites for building a “Transition Pipe”** – Since it would be an all-India network, it is important that the service provider/organization entrusted with this activity should have or be able to develop a pan-India fiber network. Therefore, large telecom service providers and ISPs are possible candidates to take up this project.
 - d. **Purpose of the Working Group** - This working group will work to plan this transition pipe, make a project report, prepare a funding model and also coordinate with the selected service provider/organization to build this “Transition Pipe” called “India6 network” which will then act as an IPv6 backbone network.
5. **“Experimental IPv6 Network” Working Group** – During the transition period, stakeholders will need an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios. This activity is not possible on an existing ISP network carrying commercial traffic. Therefore, a separate network is needed for simulating a commercial ISP network. This group will plan and build this “Experimental IPv6 Network”, which can then be used for experimentation by different vendors and organizations both from the public and the private sector. This “Experimental Network” can also be used for training of personnel for operating IPv6 networks.

6. **Pilot Project WG** – IPV6 has many capabilities which are new and not there in IPv4. These capabilities can be demonstrated through pilot projects relevant for the industry and Government. Many such applications were discussed during the IPv6 workshops conducted by TEC throughout the country. These pilot projects will provide the necessary experience for large scale implementations by the organizations. This group will plan, prepare project report, prepare the funding models and coordinate with different government and service providers to take up the deployment of such pilot projects to demonstrate the IPv6 capabilities.

7. **Applications support Working Group** – This group will facilitate the transition of existing content and applications and development of new content and applications on IPv6. It will extend its support to all member organizations. This group will consist of members from software and content developers.

8. **Knowledge Resource development Working Group** - In addition to different activities it is also important to develop the IPv6 knowledge base in the country. This knowledge base can be developed with active participation of the educational institutes. The members of this working group will be drawn from educational institutes, who will be actively involved in the change of curriculum to include IPv6 as a subject, pursue with the Ministry of HRD to take up study of IPv6 related issues by educational institutes, involve in basic research on IPv6 etc.

9. **IPV6 implementation in the Government Working Group** - This working group will pursue with different government departments for implementation of IPv6. The members will be drawn from nodal officers in various government departments. It will be headed by the concerned DDG of Dedicated Unit.

5.6 Distribution of Working Groups between Different Service providers

It is proposed to distribute different activities of the working groups between different service providers as given below –

Table 5: Allocation of Working Groups to Service Providers / Organizations

Sr.No.	Name of the Working Group	Proposed Lead Service Provider / Organization
1.	Training and Awareness WG	
2.	Action Plan and IPv6 Network Implementation WG	
3.	Standards and Specifications Working Group	
4..	India6 Network WG	
5.	Experimental IPv6 Network WG	
6.	Pilot Project WG	
7.	Applications support WG	
8.	Knowledge Resource Development Working Group	
9.	IPv6 Implementation in the Government Working Group	

5.7 Human Resource Requirements

IPv6 expertise, both technical and non-technical would be required at different levels. It is not expected that all the expertise would be available in one organization. So experts will have to be brought into the Task force both from within the government and outside the government. Depending upon the existing availability of required manpower, the following methods would be adopted for sourcing the manpower –

- a) Internal sourcing
- b) External sourcing
- c) Deputation from other govt. departments / PSUs / private sector organizations

The selection of the manpower to conduct the activities of the working group will be done by the lead organization. The lead organization will try to give due representation to all the participating organizations.

5.8 Funding Model and Budget Requirements for the Task Force

The funding of the activities of the Task Force will be based on the “Public Private Partnership” model where contributions will be made both by the government and the participating organizations. Funding will be required at the following levels –

- a) Activities of the Oversight Committee
- b) Activities of the Steering Committee
- c) Activities of the Working Groups
- d) Task Force Secretariat

For running the activities of the Oversight Committee, Steering Committee and Task Force Secretariat, responsibility shall be taken up by the IPv6 Task Force Secretariat. Delegation of adequate financial powers shall be given for this purpose.

For the activities of the individual working groups, funding will be done by the lead organization. The government contribution can vary and shall be decided on case to case basis on the recommendations of the respective working group. As an incentive, the lead organization (and the government) in the working group will have first right on any kind of intellectual property, which arises out of the activities of the respective working group. The working groups will be permitted to charge fees for the services rendered by them to different stakeholders. The scope of activities and funding pattern will be guided by a “Memorandum of Understanding” between the lead organizations and the government.

Annual budget of the Task Force containing the details of contributions by the sponsoring organizations and the contribution from the government will be approved by the Oversight Committee. The approved budget will be put up to the Government for demand of grants. The details of the budget requirement shall have to be worked out separately in association with the lead organizations. *The decision of lead organizations, scope of activities and funding pattern for various working groups shall be taken up in the first meeting of the Oversight Committee soon after formation of the IPv6 Task Force.*

5.9 Creation of “Indian IPv6 Centre for Innovation” as a Long term alterative to Task Force

Transition from IPv4 to IPv6 will not happen overnight. Organizations have invested lot of money in building the IPv4 infrastructure over the years and replacement of that infrastructure is not feasible without the recovery of the investment. Therefore, IPv4 and IPv6 will co-exist for a long time to come. During the intervening period the organizations will have to face many hurdles during the process of transition since IPv6 is a new protocol and research is still going on throughout the world to understand and exploit its numerous capabilities.

Since there are critical activities needed for successful deployment of IPv6, other countries have taken many initiatives in building dedicated institutions for coordinating all the activities associated with the deployment of IPv6. Some have created “Task Forces” and some have created dedicated centers, some have created projects. In many ways, countries have adopted IPv6 in their own ways.

The long term solution to tackle all IPv6 related issues in the country is to set up a dedicated institution as an alternative to the Task Force. It can be called the Indian IPv6 Centre for Innovation. The details of the proposed IPv6 centre is given in Chapter-8.

5.10 Actionable Points

1. Creation of the IPv6 task Force with the structure and functions mentioned therein
2. Creation of “Indian IPv6 Centre for Innovation” as a long term measure to take over all the functions of Task force on IPv6 deployment
3. Assignment of lead organization to each of the working groups in the task force, which can be decided during the first meeting of the Oversight Committee after the formation of the Task Force.

-----x-----

	6
--	----------

<p>IPv6 Standards and Certifications</p>

6.0 Introduction

IPv6 is sometimes also called the Next Generation Internet Protocol or IPng. IPv6 was recommended by the IPng Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994 in RFC 1752, The Recommendation for the IP Next Generation Protocol. The recommendation was approved by the Internet Engineering Steering Group and made a Proposed Standard on November 17, 1994. The core set of IPv6 protocols were made an IETF Draft Standard on August 10, 1998.

The “IPv6 Forum” is the apex body in the world which is spearheading the IPv6 movement in different countries. It is also taking proactive steps in the development of specifications and test tools for doing the conformance and interoperability tests for Ipv6 equipments. It is making all efforts to develop common specifications and standards which can be used by different countries and organizations throughout the world. To assist in these activities the IPv6 Forum is supported by many organizations and projects throughout the world.

6.1 Japanese initiatives in development of specifications

Japan’s foray into the Internet domain started with the WIDE project almost 20 years ago. The basic philosophy of the Widely Integrated Distributed Environment (WIDE) Project lies in the provision of a global connection between computers and all other equipment and the construction of a distributed system that will serve a useful purpose from an individual and social viewpoint and to bring to the fore the relative issues and problems in order to bring this to fruition. This philosophy has existed since the project was launched in 1988 to the present day amidst remarkable developments in network technologies. The Project aims to construct a highly public information infrastructure that will contribute to society in a variety of fields including medicine, finance, education and law.

6.2 Several Successful efforts under the WIDE Project for IPv6

- (i) **KAME** – created the first (and still reference) IPv6 stack implementation. This was done in FreeBSD (due to its having one of the best and most mature TCP/IP implementations). It was quickly ported to OpenBSD and NetBSD. These platforms have been used to host many IPv6 applications and are included in many IPv6 compliant applications.
- (ii) **USAGI** – project similar to KAME to create a quality IPv6 stack for Linux. Many Linux distributions (from 2.6 Kernel onward) now include the USAGI stack, which is dramatically better than the original IPv6 support in Linux.
- (iii) **TAHI** – project to create high quality and exhaustive test suites for IPv6 based applications and products. These test suites (for the Phase 2, or “Gold” level) test every aspect of every relevant IETF RFC (Conformance Tests) as well as interoperation with at least four distinct IPv6 based products.

6.3 The TAHI Project

The TAHI project (which is a part of the WIDE project) is a joint effort of many organizations, mainly with the objective of developing and providing the verification technology for IPv6 compliance. The TAHI project researches and develops *Conformance tests* and *Interoperability tests* and also the various test tools. They work closely with the University of Tokyo, Yokogawa Electric Corporation, KAME project and the USAGI Project. To develop the test specifications active experimental scenarios are created through test events. The IPv6 forum and TAHI, Japan together have organized many IPv6 Interoperability test events in the past. These events provide an important platform where different IPv6 vendors come together and test their equipments against each other for interoperability. During the test event testing scenarios are built separately for “Hosts” and “Routers”. The test results in these events help not only the vendors but also TAHI to refine the specifications for IPv6 compliance.

6.4 Certification of Products (IPv6 Ready Logo Program)

The most significant contribution of TAHI has been to the IPv6 Ready Logo program of the IPv6 Forum. The IPv6 Ready Logo program is an international testing program intended to

increase user confidence by demonstrating that IPv6 is currently available for today's deployment and use. The key objective and benefit of the IPv6 Ready Logo program is three fold;

- Verify protocol implementation and validate interoperability of IPv6 products.
- Provide access to free self-testing tools.
- Provide IPv6 Ready Logo testing laboratories across the globe dedicated to provide testing assistance or services.

The IPv6 Ready Logo program works under the aegis of the IPv6 Forum. The IPv6 Forum created the IPv6 Ready Logo Committee in 2002 to manage this globally unique logo program.

6.5 IPv6 Ready Logo Committee

The IPv6 Ready Logo Committee manages the IPv6 Ready Logo Program. It is presently headed by Mr. Hiroshi Esaki, Professor, Tokyo University and also the Chairperson of the IPv6 Ready Logo Committee. The IPv6 Ready Logo Committee assists vendors with the IPv6 Ready Logo testing and application requirements. For this purpose it approves various testing laboratories throughout the world for conducting the tests specified by the IPv6 Ready Logo Committee. These are the “IPv6 Ready Testing Centers”. They can test products using the TAHI test suites, and submit the results to the IPv6 Ready Logo Committee, whose Chair can accept the results and certify the product or application as compliant and interoperable. Current IPv6 Ready Logo testing centers include:

- Japan: Japan Approvals Institute for Telecommunications Equipment (JATE)
- USA: University of New Hampshire InterOperability Lab (UNH-IOL)
- France: IRISA/INRIA
- Korea: Telecommunication Technology Association (TTA)
- China: Beijing Internet Institute (BII)
- Tawian (ROC): ChungHwa Telecomm Labs (CHT-TL)
- Infoweapons Corporation, Phillipines

To become one of the recognized testing labs of the IPv6 Forum the participating organization should have adequate testing and certification facilities for giving service to the vendors. The facilities will be audited by the IPv6 Logo Committee (v6LC) with the help of their technical teams. The v6LC has prescribed a code of conduct for all its members and the prime objective of the code of conduct is to maintain neutrality and work for the betterment of IPv6 specifications development.

6.6 Different Phases of the IPv6 Ready Logo Program

The program has 2 phases -

- a) **Phase-1** – The Phase-1 program is the “Silver Logo” in which a minimum number of prescribed tests have to be passed by the equipments to be eligible for becoming IPv6 ready and receive the silver logo. Once equipment receives the silver logo it means that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations. The Phase-1 core protocols include IPv6 Specification, Neighbor Discovery, Address Auto-configuration and Internet Control Message Protocol (ICMPv6). The Phase-1 test coverage includes approximately 170 tests.
- b) **Phase-2** – The Phase-2 Gold Logo started in 2005. In this phase the equipments have to pass through more tests. The Gold Logo indicates that a product has successfully satisfied strong requirements as stated by the IPv6 Ready Logo Committee (v6LC). These tests cover the MUSTs and SHOULDs in the IETF RFC tested. The Phase-2 IPv6 core test coverage includes approximately 450 tests. The IPv6 Forum **strongly encourages** vendors to obtain the IPv6 Ready Logo Phase-2. The Phase-2 Logo verifies optimum compliance because of the complete series of tests including the "MUST" and the recommended "SHOULD" for the IETF specifications tested.
- c) Many countries are now accepting these certifications (especially the Gold level) as proof that the products are compliant and faithfully implement the all relevant standards. Some countries require such certification before products can be purchased for use in their government agencies. The two approval lists can be found at:

- i. http://www.ipv6ready.org/phase-1_approved_list (for Silver)
- ii. http://www.ipv6ready.org/phase-2_approved_list (for Gold)

6.7 Writing Test Specifications

The IPv6 Ready Logo test specifications are currently developed by the following organizations..

- (i) TAHI Project - Japan
- (ii) UNH-IOL (University of New Hampshire InterOperability Laboratory)- US
- (iii) IRISA - France - European Laboratory for Interoperability testing Internet protocols
- (iv) CHT-TL - Taiwan - IPv6 Ready Logo Testing Lab - ChungHwa Telecom Labs
- (v) BII - Beijing Internet Institute - China - IPv6 Ready Logo Testing Lab
- (vi) TTA - Korea - Telecommunication Technology Association IPv6
- (vii) JATE - Japan Approvals Institute for Telecommunications Equipment

6.8 Certification of services (IPv6 Enabled Logo Certification for ISPs)

The IPv6 Ready Logo Program also provides compliance testing for ISPs that offer IPv6 or Dual Stack Internet service. For details see the IPv6 Enabled Logo program at http://www.ipv6forum.org/ipv6_enabled/

Malaysia has already certified 9 ISPs through this program, which will shortly be offering commercial service.

6.9 US Initiatives in the Development of Specifications (USGv6 / NIST IPv6 Testing)

The U.S. is so far alone in creating their own IPv6 product compliance profile (by NIST, the National Institute of Standards and Technology). The details of this are available at <http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>

USGv6 testing is a superset of the IPv6 Ready Logo program, and is based heavily on (“harmonized with”) the tests developed by TAHI. However, to obtain the NIST certification (USGv6), the testing must be done at NIST approved labs, including UNH-IOL (above) and ICSA Labs (part of Verizon). USGv6 certification is now required to sell IPv6 products to U.S. government agencies.

Other countries will accept IPv6 Ready certification done by any IPv6 Ready Testing Center. It is even possible for technically advanced vendors to run the TAHI certification tests themselves and submit the results to the IPv6 Ready Logo committee. Assuming everything is in order, the same certification is granted as to products tested by an IPv6 Ready Testing Center.

6.10 Recommendations for India

- (i) **Development and adoption of IPv6 specifications** – We may adopt the specifications developed by the *IPv6 Ready Logo* under the IPv6 Forum since these specifications ensure worldwide interoperability. However, there may be country specific requirements also depending upon the local environment. **TEC shall develop the IPv6 standards and specifications for the country based on the IPv6 Ready Logo Standards and specifications and our country’s local requirements. The final set of specifications thus prepared shall be followed by all service providers and concerned industries for deploying their IPv6 equipments in the country to meet out the Conformance, Interoperability and other requirements.** Therefore, if vendors have obtained the “IPv6 Ready Logo certification” they will have to conform only to the additional specifications developed by TEC for full compliance of the specifications developed by TEC.

- (ii) **Recognition of the IPv6 Lab set up by TEC** – The IPv6 Ready Logo has recognized many labs throughout the world to conduct various tests for conformance and Interoperability of IPv6 Equipments. **The IPv6 Lab being set up in TEC will also attempt to get such recognition as it would give the IPv6 lab due visibility at an international level.** This will help TEC to actively participate in the specification

development process and the lab can be utilized by all international vendors for testing purpose also.

- (iii) **Creation of facilities to provide live IPv6 environment** – In India, TEC is setting up a “**Testbed**” for testing the vendor equipments and certifying them for IPv6 compliance. It will have a “**fixed operating environment**” fine-tuned only for “**Testing and Certification**” of vendor equipments. As per Japanese nomenclature, this is a “Testing Center”. The TEC “Testbed” is not meant to be used for simulation of live IPv6 environments e.g. it is not to be used for simulation of a large-scale ISP using IPv6. Moreover, it is not possible to use a live IPv6 network of an ISP for experimentation. **Therefore, there is a need to create separate facilities for simulating the live IPv6 environment. This is necessary because then only different vendors can bring their IPv6 equipments to test how they will interoperate and perform under live conditions.** It will also aid in the certification of IPv6 products.
- (iv) **Creation of more IPv6 Ready Testing Centers** - These can be created within an industry association (TTA in Korea, JATE in Japan and ETSI I EU). It can also be created as part of a private sector company (BII in China and UNH-IOL in the USA). In some cases, it is part of a major Telco (CHT-TL in Taiwan). It could in theory be run by a government agency also. The proposed India IPv6 task force/National IPv6 centre shall involve all stakeholders in India for creation of more such testing centres across the country for the benefit of service providers and manufacturers
- (v) **Enabling legislation for mandatory certification** - The government shall mandate IPv6 certification of products so that vendors and purchasers supply and deploy only IPv6 compliant products. Such a government mandate can greatly incentivize vendors to support IPv6 and obtain such certification in their products.

6.11 Actionable Points

1. TEC will develop the standards and specifications for IPv6 conformance and Interoperability tests in association with the IPv6 Ready Logo program of the IPv6 Forum
2. These standards and specifications will be followed by all stakeholders for deploying IPv6 compliant equipments and services in the country.

-----x-----

	7
IPv6 Adoption: A New Way Ahead	

**IPv6 Adoption:
A New Way Ahead**

7.0 Introduction

Deployment of IPv6 around the globe is increasing and along with it applications, which can be more easily deployed using IPv6. Convergence is now here with mobile, data, voice and video all going over Internet infrastructure. Some of the new features of IPv6 as compared to those of IPv4 are

Table 6: Advanced features of IPv6

Vastly increased address space	Extending the 4 billion IPv4 address space to the 3.4×10^{38} IPv6 address space allows many existing and new processes to receive addresses. This includes all the world's billions of mobile phones and computing devices. It will also include the nearly 200 addressable processes in a typical motor vehicle. Homes may have tens or hundreds of IP addresses. It has been said that in the future, any device worth more than \$10 will have at least one IP address (source: Dr. Dean Economou, CENTIE 2002).
Autoconfiguration	Autoconfiguration is the automatic configuration of devices without manual intervention, software configuration programs or jumpers, and devices should just "Plug and Play". When an IPv6 network adapter card is activated, it assigns itself an IP address based on a standard prefix appended to its own MAC address. This enables the device to communication on the local network and seek out any servers that it is allowed to communication with. These might use DHCPv6, AAAA or other mechanisms to download gateway addresses, security setting, policy attributes or other relevant services. This process also includes duplicate address detection, multihoming and other useful network administration activity.
Default IPsec Security	IPv4 was developed at a time when Security was not uppermost as a concern. Authenticating protocols such as IPsec were developed later

	<p>and need to be retrofitted into IPv4 protocol stacks. This leads to interoperability and implementation inconsistencies. IPv6, on the other hand, had security as a major design criteria and conforming standards-based IPv6 protocol stacks have IPsec as a mandatory requirement. All conforming IPv6 sessions can therefore be authenticated. This is not to say that users cannot control whether to use this or not, however the capability is there for everyone.</p>
<p>End to end trust</p>	<p>Network Address Translation (NAT) has broken the end to end trust that was a hallmark of early IPv4 services. As there are one or more translation devices in most of today's Internet connections, there is no visibility between the end-users themselves. The authenticated IPv4 Internet connections stop at these NAT gateways. There can be one or thousands of users behind these gateways and the A party has no way of knowing about them, let alone trusting them. Authenticated IPsec IPv6 sessions will route from end to end. Users and machine-to-machine communication sessions will have confidence that the party/service they are connected with is genuinely who they think it is.</p>
<p>MobileIPv6</p>	<p>When a device moves from its home network, its IP address will be recognized as a foreign address in its new location and will be denied service. The gateway it originally was told to use in its home network is no longer valid and communication sessions will not be established. This may happen many times in the course of a single journey, across a city for example, where many different carrier services might be available. To overcome this limitation, a process called MobileIP was developed in IPv4. This consisted of the devices calling 'home' and telling the home network of its changing gateway environments (the foreign correspondent model). This is a very inefficient way to operate as all traffic to and from the mobile device has to be routed via the home network. MobileIP has been extended in IPv6 to overcome this inefficient triangulation. In MobileIPv6, a foreign correspondent server is continuously updated as to the network the device is in and which</p>

	gateway to use to reach the traveling device. The bulk of the packets flow directly between mobile device and its communicators, and not via the home address. This vastly improves performance and reliability, and reduces cost.
Flow Label QoS	All of the Differentiated Services (DiffServ) and Integrated Services (IntServ) Quality of Service attributes from IPv4 are carried over into IPv6. In addition, IPv6 exclusively has a 20-byte Flow Label field. This field is being developed to provide a rich set of Quality of Service attributes for the growing IPv6 world. Many of these sets are being deployed, and market acceptance/adoption will determine the ones that succeed.

The advantages of these features unique to IPv6 are that they promise to deliver an entirely new breed of applications and services which are not possible to be delivered using IPv4. It is possible for different government departments and also organizations in the private sector to take up such applications, initially as a pilot, thereafter in full commercial deployment. Some of these applications are discussed here.

7.1 Logistics and Supply Chain in Indian Railways

The Indian railways have the largest logistics and supply chain network in the country consisting of wagons, bogies, engines, processing centers, point of sale terminals , millions of parcel objects each day. It is possible to build a suitable logistics and supply chain network using IPv4 also but then such a system cannot be expanded in future due to exhaustion of IPv4 addresses. Secondly, such a system would be very difficult to integrate with RFID tracking.

However, IPv6 has innovative features built into the protocol like autoconfiguration etc. Coupled with the large number of addresses available, it would be far simpler to build such a system using IPv6.

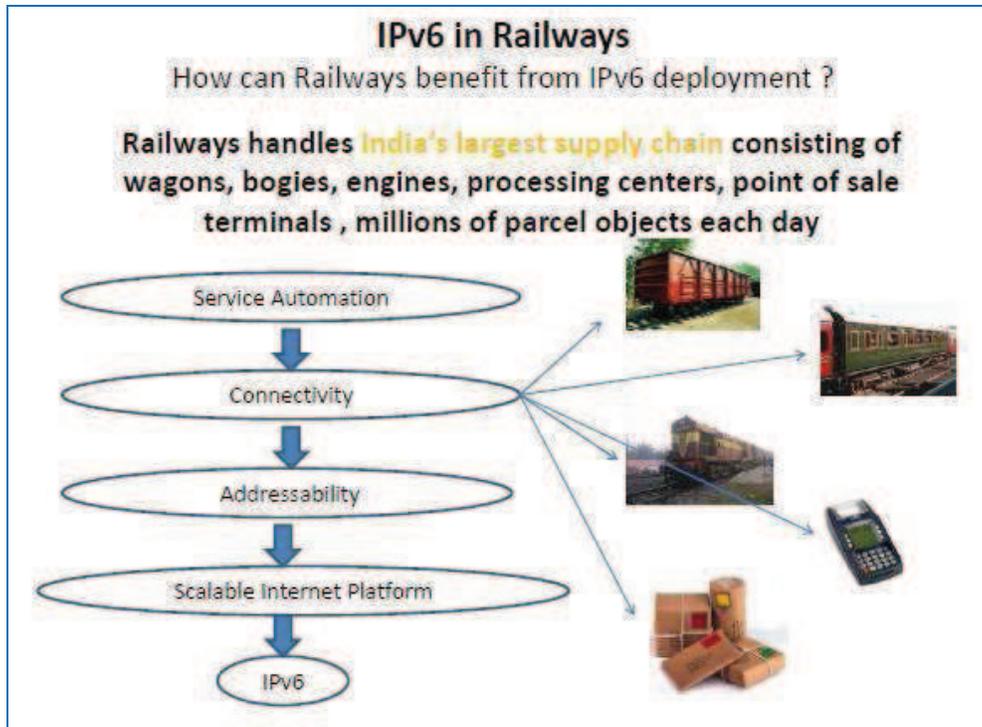


Figure 11: Schematic of IPv6 Implementation in Railways

The large address space and autoconfiguration features will help implement RFID tracking of goods in the system. This can not only improve the customer service by reducing the transit time but also help in faster tracking of lost goods.

Similar approach can be adopted by other organizations also for improving their logistics and supply chain by using IPv6.

7.2 Intelligent Transport System

Traffic monitoring and management is one of the most crucial issues being faced by metropolitan cities in India. The citizens need to get real-time view of the traffic condition in different parts of the city so that they can plan their commute. Similarly the public service vehicles like roadways buses, school vans, ambulances, fire brigades, police petrol vehicles etc. need to be monitored and their real time location and availability needs to be communicated to the citizens.

Simulation models tested with real data can also be used to predict the expected time to clear the traffic congestion and this information can be revised on real time basis.

Techniques involving signaled diversions at the key junctions around the source of the jam and the periphery of the congested area can be implemented to mitigate the traffic congestion.

It is possible to implement such a system using sensors, video cameras, signaling points etc. communicating and exchanging information through an IPv6 based network. A schematic of such a system is shown below.

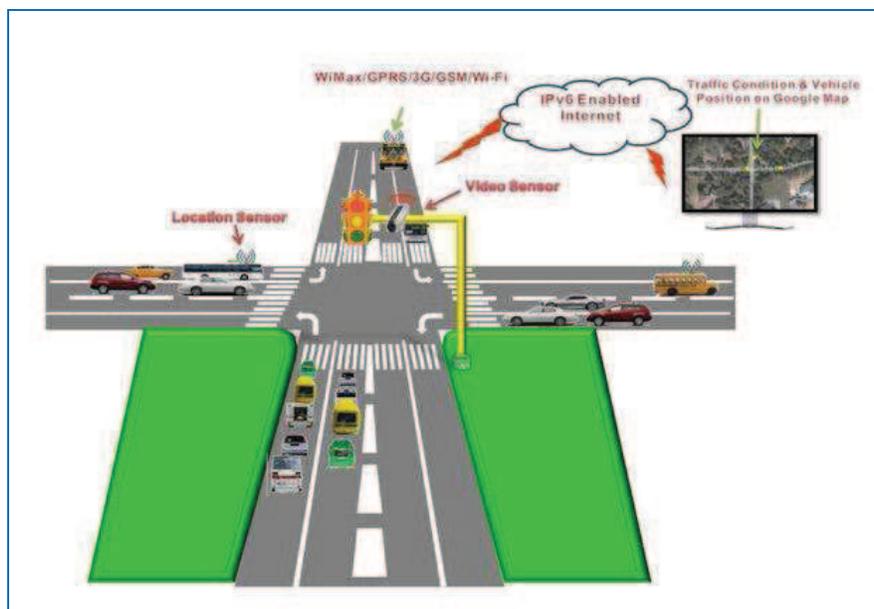


Figure 12: Schematic of Intelligent Transport System

IPv6 is a natural choice for implementing ITS because of the following reasons –

- ITS needs a large address space: millions of vehicles with multiple devices each requiring a public global address which can be provided by IPv6 only.
- ITS needs the advanced features provided by IPv6 like Mobile IPv6 and enhanced security.

The traffic will be monitored using IPv6 Video Sensors installed at the red light crossings. They will provide real-time traffic condition. Similarly IPv6 Location Sensors will provide real-time location of all public service vehicles. The real-time locations of public service vehicles and traffic conditions will be displayed over the web using Google Maps.

7.3 Rural Emergency Health Care

The healthcare services in India are heavily biased towards the urban areas both in terms of infrastructure and the availability of services. Some of the key critical aspects which

contribute here are the lack of availability of Secondary and Tertiary care facilities in the rural areas. Even the primary health care is at times elusive in the rural areas. In the rural areas, we have the Doctor to population ratio lower by 6 times, and the beds in rural hospitals to population lower by 15 times. This has resulted in the health care costs rising in the rural areas, wherein villagers are spending about 1.5 times more than their urban counterparts for the treatment of the same illness.

Technology can, however, bridge the gap to some extent, if not completely. IPv6 is one such technology, which can make a difference in Telemedicine and Emergency Health Care. Some of the key features and aspects of IPv6 technology which help implement Tele-medicine in a better way are:

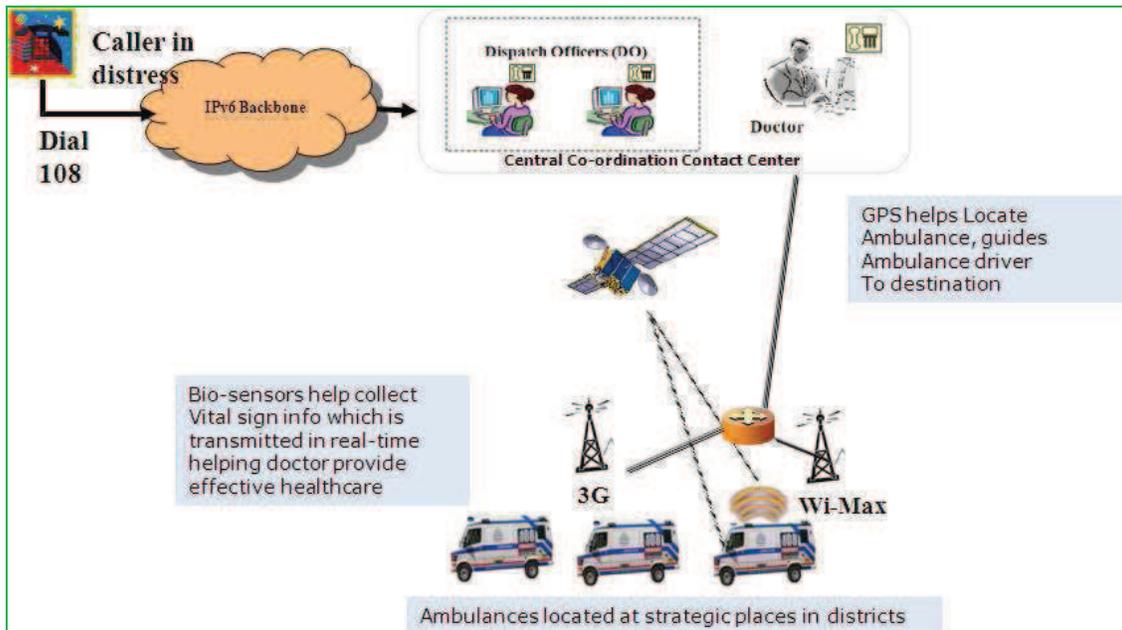
Table 7: IPv6 Technologies – Enabling Next-Gen Healthcare	
IPv6 availability on all communication technologies – 3G, WiMax, PAN ...etc	Single protocol for diverse communications needs as Ambulance traverses across the Rural region. Single protocol right from Bio-sensor to Doctor’s console
IP Addresses	Need for large number of IP addresses – by Bio-sensors, Routers, Inventory tracking system ...etc.
Mobile IPv6	Ensures that seamless sessions are maintained for various entities as Ambulance moves across various regions
Peer-to-peer connection	Provides the feature wherein end-to-end sessions for Bio-Sensors are maintained from Ambulance to Doctor’s console
Multimedia transmission - Optimized Always-on-Realttime network	Optimized Real-time transmission capabilities help provide – Real time Video conference and VoIP facilities, using very simple and low cost equipment
End-to-end Security	Healthcare information security is a critical issue in wireless networks. It becomes all the more important when the network is being utilized by medical applications. IPv6 offers enhanced security features that make it appropriate to be used for medical biosensor wireless communications networks
Auto-configuration	Multiple devices in Ambulance – simplifies network Management of devices in Ambulance

Some of the key IPv6 capabilities and how, they would help in improving the Emergency Healthcare management are given below –

Table 8: Technologies for Healthcare

IPv6 based Technology	Details
Bio-Sensors	Collect Vital sign details about Blood Pressure, ECG, Temperature ...etc
IPv6 based Real-time Vital signs data transfer	Transmits real-time information over low bandwidths
Seamless Video-Conference	Low cost Video conf system – providing seamless visual experience
VoIP enabled Telephony	VoIP telephony making use of existing Datacom Infrastructure
Automatic Vehicular Location System	Vehicle location system making use of the triangulation information from Cellular Service Provider
Real time Inventory Asset and Inventory tracking using IPv6	Sensor based Ambulance Inventory and Asset tracking

Figure 13: An IPv6 based Emergency Health Care System



An IPv6 enabled Emergency Healthcare system shown above, will help provide real-time diagnosis and medical support during ambulance transport. The new telemedicine program will allow physicians to begin treatment as soon as a patient is taken into an ambulance. This enables the remote experts to support and guide the mobile crew and the hospital to be prepared before the ambulance end up at the hospital. The IPv6 system will transmit patient bio-signals and Video from a moving ambulance and deliver it to the desktop computer of Doctor at the Contact center. It should be able to support Real time data sharing, ability to give remote prescriptions and support bi-directional messaging.

7.4 Smartgrids for Power Distribution

India, a unique and a developing country with huge population, provides many opportunities for Greenfield application deployments. One of such applications for India is the Smart Grid for the Electric Utilities. Smart Grid provides smooth and efficient delivery of electricity from suppliers to consumers using two-way digital communication technology to save energy, reduce cost and increase reliability. Smart Grid is being promoted by many

governments across the world as a way of addressing the global warming and emergency resilience issues.

IPv6 is a natural choice for building Smartgrids because IPv6 is a transport protocol for interconnecting heterogeneous physical links (IEEE 802.15.4, IEEE 802.11, Ethernet, WiMAX, Cellular Networks, etc), and can transfer any type of information (Voice, Multimedia, Data, Real-time information etc.). IPv6 can handle any data rates from few octets per day to Gigabits per second thereby making it highly flexible. Given below is a typical IPv6 based smartgrid infrastructure.

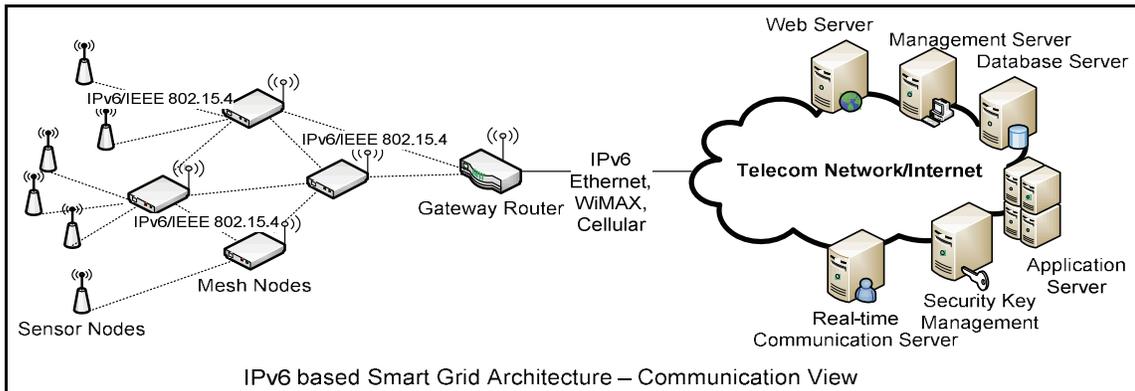


Figure 14: IPv6 Based Smartgrid Schematic

Electric Utilities can implement Smart Grid infrastructure and services based on IPv6 with low cost of ownership. Implementation of IPv6 based networks for Greenfield applications is much easier and supports Smart Grid evolution for the foreseeable future needs. Hence, for Utilities adapting IPv6 as the base transport protocol, IPv6 is key for the future of the Smart Grid.

-----X-----

	8
Indian IPv6 Centre for Innovation	

Indian IPv6 Centre for Innovation

8.1 Introduction

Migration from IPv4 to IPv6 will not happen overnight. Organizations have invested lot of money in building the IPv4 infrastructure over the years and replacement of that infrastructure is not feasible without the recovery of the investment. Therefore, IPv4 and IPv6 will co-exist for a long time to come. During the intervening period the organizations will have to face many hurdles during the process of migration since IPv6 is a new protocol and research is still going on throughout the world to understand and exploit its numerous capabilities.

Since there are critical activities needed for successful deployment of IPv6, other countries have taken many initiatives in building dedicated institutions for coordinating all the activities associated with the deployment of IPv6. Some have created “Task Forces” and some have created dedicated centers, some have created projects. In many ways, countries have adopted IPv6 in their own ways.

8.2 Similar Initiatives in Other Countries

1. **Japan IPv4 Exhaustion Task Force** – The Japanese Government has designed its latest program around the concept of ubiquity called “u-Japan” (Ubiquitous Japan) as the 2010 ICT Society platform. It is centered on empowering the Japanese end-user:

- i. Ubiquitous access, connecting everyone and everything
- ii. Universal and user-friendly
- iii. User-Oriented
- iv. Unique, be something special

The Japanese government created a concerted forceful effort by combining global initiatives to work for their vision to become the Most Advanced IT Nation in the world. Japan created the “**IPv4 Exhaustion Task Force**” to coordinate various industry efforts to migrate to IPv6 before IPv4 exhaustion by JPNIC in 2011. It

supported the creation of the IPv6 promotion council and created a public-private partnership.

China Next Generation Internet - China has instituted a full adoption policy of IPv6 by creating the China Next Generation Internet budgeted with over 170 million \$. The Chinese government created a group of eminent personalities along with the IPv6 Forum, which recommended the adoption of IPv6 in the CNGI project to the Chinese government that will be by far the largest commercial backbone ever-built from scratch for a single technology. His backbone will become the glue for all services in China for fixed, mobile, GRID and research.. China has shortened its gap with developed foreign countries by developing the Next Generation Internet while at the same time challenges are rising up, which require continuous exploration and innovation.

2. **USA** – The US DOD has demonstrated leadership by announcing support for Ipv6 back in June 2003 after lengthy discussions and recommendations of the Ipv6 Forum and the **North American Ipv6 Task Force**. The military sector responded immediately with support from the German and French Ministries of Defence who did their homework independently and are now cooperating together. The North American Task Force has done many pioneering work in the USA. E.g. Moonv6 www.moonv6.org is an international project led by Nav6TF to execute deployment testing of Ipv6 technology. It is jointly implemented by commercial service providers, UNH- IOL, Government organizations, academic entities and network equipment vendors. Test items are determined by network operation requirements of the US Government Agencies and commercial service providers. Nav6TF has also started the Metronet6 project which is an emergency responder network concept built using Ipv6. It is a 24x7x365 ad-hoc mobile network that integrates E911, Internet, and voice on a common Ipv6 infrastructure. For city-to-city and state-to-state communications the current Nav6TF Moonv6 project can provide an Ipv6 native backbone peering network to be used.

3. National Advanced Ipv6 Center, Malaysia

- (i) The National Advanced Ipv6 Centre (Nav6) was established by the Ministry of Energy, Water and Communication (MEWC), Malaysia in March 2005 . It serves as the National Centre for Ipv6 research, human resource development and monitoring of Ipv6 development for Malaysia. As part of its mission, Nav6 plans and implements appropriate programs in order for Malaysia to be an Ipv6 enabled nation by 2010. The Malaysian government has entrusted Nav6 with the mission to develop the National Ipv6 Roadmap . The Roadmap will be the blue print that will be used by the country to implement the migration of its network to Ipv6. The Roadmap was completed and submitted to the government in March 2008.
- (ii) Nav6 started working with two government agencies in their pilot implementation of Ipv6 networks in early 2008. The rest of the agencies will also migrate to Ipv6 networks in accordance with the Roadmap.
- (iii) On human resource development for Ipv6, the Certified Network Engineer for v6 (CNE6) and Certified Network Programmer for v6 (CNP6) courses were developed by Nav6. They started to conduct these 101ertification training courses in 2006 to provide comprehensive knowledge and skills on Ipv6. These structure courses are endorsed by the Global Ipv6 Forum which Nav6 or its partner will conduct at least once every quarter.
- (iv) In addition to training and Ipv6 consultancy, Nav6 also provides other services such as network security audits for ISPs and collaboration on information technology related research and development.
- (v) The main focus of the Nav6 is the promotion of Ipv6 and support government agencies and other organizations in Malaysia and also the ASEAN region in their migration to Ipv6. The Table below gives the various focus areas of Nav6 for Ipv6 deployment.

8.3 Development in India

Presently, TEC has been entrusted with the task of guiding the country to migrate from IPv4 to IPv6. However, since the migration process is complex and it has to happen

with the active participation of all stakeholders and at present there is practically no other institution in India to oversee all the activities related to the deployment of IPv6 in India. Creation of the “**India IPv6 Task Force**” is only a short term solution to push the industry forward so that it is ready to deploy IPv6 before 2012, by which time APNIC would have exhausted all its IPv4 addresses. The long-term solution is to create a dedicated organization to take over all the activities of the task force and also continue to address new IPv6 related issues faced by the country in future, fully involve itself in the R & D activities of this protocol including development of different applications and to see that all IPv6 related applications are fully deployed and utilized in the country.

Therefore, it is proposed that India should have a dedicated National organization for coordinating and development of all IPv6 related issues in the country.

8.4 Proposed Activities of the “Indian IPv6 Centre for Innovation”

1. **Training and Awareness** – This will be an important activity of the center. It will conduct training programmes, seminars, workshops, awareness campaigns, certificate courses on IPv6-based technologies etc. We can have some conservative estimates about the manpower required to be trained for deploying IPv6 based networks in future.
 - i. In Central government there are about 100 different departments and ministries. Each department may have 100 different units/branches/subordinate offices etc. Even if each department/ministry needs 5 persons, requirement of IPv6 trained personnel would be about 50,000.
 - ii. Similarly in state governments, we have 34 states/union territories. Each state has about 100 subordinate departments/units etc. So if each unit requires at least 5 persons, then requirement is about 17000.
 - iii. In addition there are about 250 Central PSUs, having numerous branches/units/subordinate offices throughout the country. On an average if each PSU has about 100 subordinate offices with each subordinate office needing about 5 engineers, the requirement would be 1,25,000

- iv. In addition to above we also have large number of State PSUs. We also have the demand from the private sector. Let us say there the demand is another 100,000 personnel.

So even by most conservative estimates, we need at least 350,000 personnel trained in IPv6 within the coming years. So IPv6 training requirement of different type is very huge.

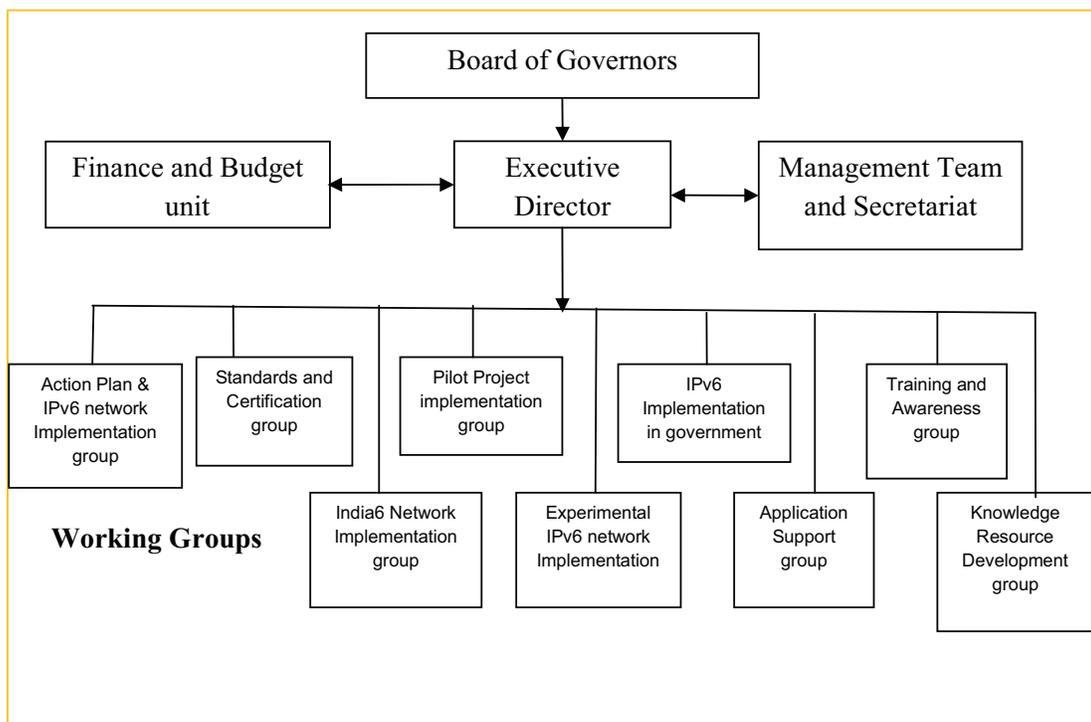
2. **Coordination with all the government organizations and also organizations in the private sector to implement their IPv6 deployment plans and find solutions to problems faced during the process of migration** – There are more than 100 different central and state government ministries, departments and PSUs. The DoT has already issued instructions to them for appointment of nodal officers for facilitating the migration from IPv4 to IPv6 in their respective organizations.
3. **Provide all the technical and managerial resources** required to build the “India6” IPv6 backbone network in the country
4. Provide all the necessary resources required to build the “**Experimental IPv6 Network**” in the country. **The network can be setup within the premises of this institution.**
5. To coordinate and share expertise with different stakeholders to implement different **IPv6 based pilot projects** in the country.
6. To actively take up **Research and Development** work in IPv6 along with the creation of necessary infrastructure. To commit to continuous research, experiment and development of new applications as well as the porting of existing applications to the new IPv6 specifications
7. Facilitate the **migration and deployment of applications and contents** on IPv6 by working with different application and content developers
8. Activities related to **development of the knowledge resources** in area of IPv6. It can coordinate will industry, educational institutions and policy makers to advise the government for actions needed to develop the right kind of manpower.

8.5 Structure of “Indian IPv6 Centre for Innovation”

Organization Structure

The “Indian IPv6 Centre for Innovation” should be setup as an autonomous body under the Department of Telecommunications, Ministry of Communications & IT, for the promotion and deployment of IPv6 in India. The functioning of the organization will be managed through a neutral body having representation from various stakeholders. This organization would become a close link between the Industry, Academia and Government to facilitate widespread deployment of IPv6 in India.

It is proposed that the Organization be operated and managed by the following setup –



- (i) **Board of Governors** – The members of the *Board of Governors* will consist of heads of service providers in the country, who will take up different activities in the working groups. It will also have members from key government departments, Industry associations, educational institutions and different industry forums. It will also have other senior officers from DoT/TEC as members. The *Board of Governors* will be headed by Secretary(T), DoT as its Chairman. Member(T), DoT and Advisor(T), DoT ,Sr.DDG,TEC shall also be members of the Board of

Governors. The *Board of Governors* will normally meet quarterly. It shall give policy guidelines and approve the annual budget of the organization. ***The Board of Governors shall have complete autonomy over the functioning of the Organization.***

- i. **Selection of members of the Board of Governors** – A committee formed by the Department of Telecommunications shall recommend the names of the members of the Board of Governors. The composition of the *Board of Governors* will be approved by the Minister of Communications & IT.
 - ii. The membership of the *Board of Governors* will be reviewed every 3 years.
- (ii) **Executive Director** – He should be a person of merit. He would be selected by a Committee appointed by the Government and with the approval of the Minister for Communications & IT. He should be a SAG level officer of the Government. He shall report to the Board of Governors. He would be assisted by different working groups to manage the daily activities of the organization. He should also act as a ‘contact point’ for all the stakeholders and should handle all relationship with the various agencies. He should also advise the *Board of Governors* on the advancements in technology and new activity areas proposed to be taken up by the organization.
- (iii) **Management Team & Secretariat Unit** – It will act as the one-point contact for all the members and groups in the Organization. It will be the nodal point for coordinating all the activities of the Organization and provide all types of assistance for its smooth functioning. The Secretariat will be headed by a Director (JAG) level officer¹ and will report to the Executive Director. Appropriate financial powers shall be delegated to meet out the expenditures by the Secretariat for smooth functioning of the Task Force.
- (iv) **Budget and Finance Unit** – This unit shall be responsible for finance, budget management and demand for grants for smooth functioning of the organization. It shall be headed by a JAG level officer of the Government who will report to the Executive Director.

¹ Keeping in view the possible future requirements the “number” of officers or the “level” of the officers may be increased.

- (v) **Working Groups** – These working groups will be cross-functional groups consisting of professionals from industry, academia and government.
- i. These working groups will work on different activity areas related to deployment of IPv6. Broadly speaking, these working groups would be on the same lines as envisaged under the IPv6 Task Force.
 - ii. A 3-member subcommittee headed by the Executive Director will approve the members of the different working groups and will sort out their routine problems. The other 2 members will be approved by the Board of Governors. For operational convenience creation, modification and dissolution of the working groups shall be done by this subcommittee.

8.6 Working Groups and their Functions

Under the Executive Director, there will be different working groups. Each working group will be responsible for specific activities associated with transition to IPv6. One of the member organizations of each working group will become the lead organization in that working group. The lead organization will be responsible for funding the activities of the respective working group in addition to other activities like place of meetings, logistics, selection of members etc. The members of each working group shall meet at least once every month to review the progress of that working group.

1. **Training and Awareness Working Group** – As already explained above there is a need for at least 350,000 IPv6 trained personnel within the next few years.

There are various types of activities like –

- a. Hands-on trainings in association with APNIC, IISc and other organizations
- b. IPv6 Certification programmes for qualified engineers
- c. Network engineers trainings
- d. Trainings for nodal officers and other concerned functionaries from government
- e. Conducting Workshops, seminars and conferences
- f. Representing the country in International conferences, seminars etc.

This working group will be responsible for conducting the above activities for benefit of all stakeholders. This WG will follow the “Train the Trainer” concept.

It will be responsible for developing the trained manpower required by different organizations in the government and the private sector to deal with the different types of IPv6 migration issues. The Working group can also explore revenue generation through the above activities.

2. **Action Plan and IPv6 Network implementation working Group** – This working group will be primarily responsible for studying the different network scenarios and come up with action plans for individual service providers / organizations. Different organizations are likely to have different network scenarios, so they will have needs unique to their organization. This group will assist them to create a tailor made action plan for them for migration to IPv6. This working group can also have “on-demand project” teams which can give on-site support or specialized assistance to organizations who need help for IPv6 deployment. TEC will be an active member of this working group as all the nodal officers appointed by different organizations for deployment of IPv6 would be interacting with TEC.
3. **Standards and Specifications Working Group** – This working group will coordinate with TEC for development of common IPv6 specifications for the country, which will be followed by all stakeholders. This working group will also coordinate with the IPv6 Ready Logo committee of the Ipv6 Forum to plan and advise different stakeholders and organizations like vendors, ISPs, Websites etc. for obtaining the IPv6 Ready Logo. This working group will also interact with other standardization bodies around the world like USGv6, NIST USA, JATE Japan, Nav6 Malaysia, etc to participate in various standards and specification development processes.
4. **“India6” Network Working Group** –
 - a. **Concept of Transition Pipe** – Most parts of the Internet are based on the IPv4 protocol. As the transition to IPv6 will happen gradually, during the transition period, islands of IPv6 networks will come up in different organizations spread far and wide. The problem is that organizations hesitate to migrate to IPv6 because they are not sure whether they will be able to send IPv6 traffic to another IPv6 network because of the absence of any nationwide “**IPv6 carrier network**” in between.

- b. **Need for a “Transition Pipe”** - This point has been often raised by service providers/associations in various workshops and meetings. They want a “Transition Pipe” for carrying IPv6 traffic from one IPv6 network to another IPv6 network. At present there is no such pipe at all-India level so IPv6 traffic remains isolated in closed networks. The absence of such a “transition pipe” is hampering the growth of IPv6 in India. There exist similar networks in all the countries, which are at the forefront of the IPv6 revolution, e.g. CNGI (China Next Generation Internet). In India also this type of network can be built and can be named as “**India6 network**”. *In fact service providers have suggested that the Government should take initiative in this area and build this “Transition Pipe”. Another perceived benefit of having the IPv6 “Transition Pipe” in place is that it would facilitate the penetration of broadband in our country, since future development of broadband in India will depend on IPv6 only.*
 - c. **Prerequisites for building a “Transition Pipe”** – Since it would be an all-India network, it is important that the service provider/organization entrusted with this activity should have or be able to develop a pan-India fiber network. Therefore, large telecom service providers and ISPs are possible candidates to take up this project.
 - d. **Purpose of the Working Group** - This working group will work to plan this transition pipe, make a project report, prepare a funding model and also coordinate with the selected service provider/organization to build this “Transition Pipe” called “India6 network” which will then act as an IPv6 backbone network.
5. **“Experimental IPv6 Network” Working Group** – During the transition period, stakeholders will need an IPv6 network for demonstrating and experimenting with different IPv6 transition scenarios. This activity is not possible on an existing ISP network carrying commercial traffic. Therefore, a separate network is needed for simulating a commercial ISP network. This group will plan and build this “Experimental IPv6 Network”, which can then be used for experimentation by different vendors and organizations both from the public and the private sector. This “Experimental Network” can also be used for training of personnel for operating IPv6 networks.

6. **Pilot Project WG** – IPV6 has many capabilities which are new and not there in IPv4. These capabilities can be demonstrated through pilot projects relevant for the industry and Government. Many such applications were discussed during the IPv6 workshops conducted by TEC throughout the country. These pilot projects will provide the necessary experience for large scale implementations by the organizations. This group will plan, prepare project report, prepare the funding models and coordinate with different government and service providers to take up the deployment of such pilot projects to demonstrate the IPv6 capabilities.

7. **Applications support Group** – This group will facilitate the transition of existing content and applications and development of new content and applications on IPv6. It will extend its support to all member organizations. This group will consist of members from software and content developers.

8. **Knowledge Resource development Working Group** - In addition to different activities it is also important to develop the IPv6 knowledge base in the country. This knowledge base can be developed with active participation of the educational institutes. The members of this working group will be drawn from educational institutes, who will be actively involved in the change of curriculum to include IPv6 as a subject, pursue with the Ministry of HRD to take up study of IPv6 related issues by educational institutes, involve in basic research on IPv6 etc.

9. **IPV6 implementation in the Government Working Group** - This working group will pursue with different government departments for implementation of IPv6. The members will be drawn from nodal officers in various government departments. It will be headed by the concerned DDG in DoT/TEC.

8.7 Initial Cost, Budget and Funding of the organization and the working groups

- (i) The initial cost of setting up the organization would be met with a capital grant from the Department of Telecommunications, Ministry of Communications & IT. Within a few years it is expected to run on a self sustained, cost recovery basis from its various activities.
- (ii) The organization will generate revenue through its various activities. However,

any shortfall in capital or revenue expenditure would be met by the government.

- (iii) For the activities of the individual working groups, funding will be done by the lead organization. As an incentive, the lead organization (and the government) in the working group will have first right on any kind of intellectual property, which arises out of the activities of the respective working group. The working groups will be permitted to charge fees for the services rendered by them to different stakeholders. The scope of activities and funding pattern will be guided by a “Memorandum of Understanding” between the lead organizations and the Organization.
- (iv) Annual budget of the Organization containing the details of contributions by the sponsoring organizations and the contribution from the government will be approved by the *Board of Governors*. The approved budget will be put up to the Government for demand of grants. The details of the budget requirement shall have to be worked out separately in association with the sponsoring organizations.

8.8 Human Resource Requirements

IPv6 expertise, both technical and non-technical would be required at different levels. It is not expected that all the expertise would be available in one organization. So experts will have to be brought into the organization both from within the government and outside the government. The organization shall have a suitable Human Resource Development (HRD) policy which should be approved by the Governing Council.

Depending upon the existing availability of required manpower, the following methods would be adopted for sourcing the manpower –

- a) Internal sourcing
- b) External sourcing
- c) Deputation from other govt. departments / PSUs / private sector organizations

Recruitment of the manpower in the Organization would be done by the Executive Director through an open and transparent selection process based on the already approved HRD policy. The decision of the Governing Council shall be final in all cases.

	9
Action Items	

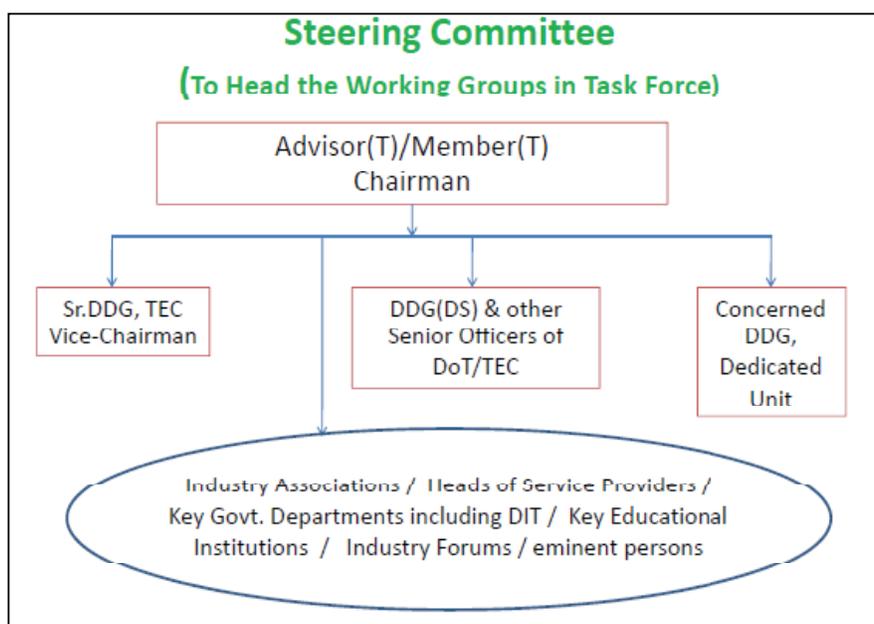
For timely implementation of IPv6 in the country the following action items have been approved by the Government-

- 1. Creation of IPv6 Task Force** - Apart from various issues discussed in the document, the most important emphasis is on the creation of a “Task Force” in India. It is through the creation of the Task Force only that timely deployment of IPv6 can be taken up with the active involvement of all stakeholders. The detailed structure and functions of the “Task Force” are explained in Chapter-5 of the document. These are briefly given below –

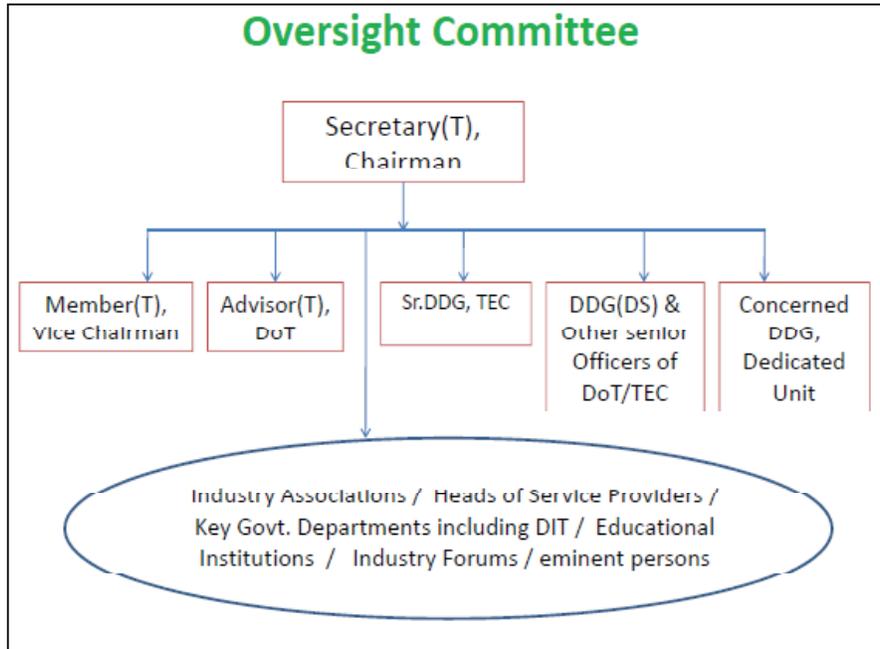
IPv6 Task Force

The task Force will be a 3-tier structure. Initially it will have 9 working groups to take up different activities related to IPv6. Each working group will have members from different organizations and one organization will be lead member of that working group. The lead organization will be responsible for all the activities of the working group, including its funding and, if required, with financial assistance from the government.

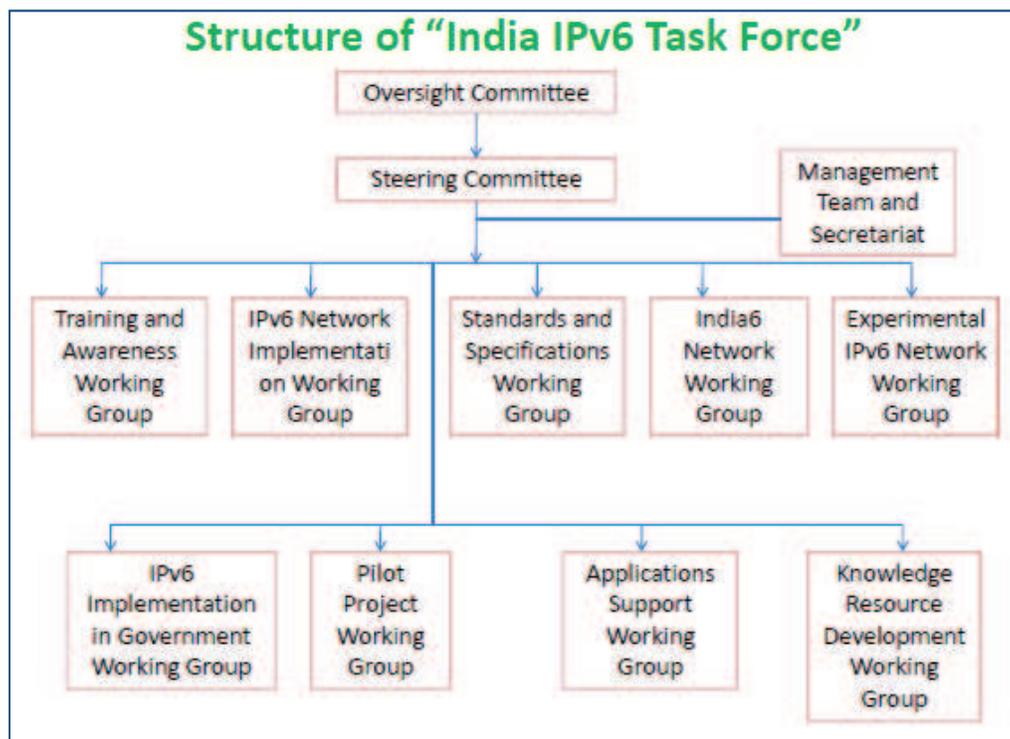
All the working groups will be headed by a Steering committee. It will oversee the activities of the different working groups. The Steering Committee will have representations from different stakeholders. The structure of the Steering Committee is given below –



The Task Force would be headed by the Oversight Committee, which will be responsible for policy making and guiding the activities of the Task Force. It would also have representation from all stakeholders. Its structure is given below



The overall structure of the Task Force is given below –



The activities of the Task Force will be assisted by a “Management Team and Secretariat”, headed by a JAG level officer.

2. **Transition Plan for Central and State Government Departments** – One of the working groups of the Task Force will coordinate with nodal officers of different government departments to assist them in the preparation of their transition plans. A schedule for transition to IPv6 by all the government departments has been suggested in the document for transition by March-2012. **All central and State government ministries and departments, including its PSUs, shall start using IPv6 services by March-2012.** Actual details for individual organizations can be worked out by the working group if required by the concerned organization. This working group will be headed by the concerned DDG of the Dedicated Unit and other members will be from other ministries / departments.
3. **Transition Plan for all service providers** - Large service providers have already initiated the transition process. Most of the service providers have not committed to become ready for handling IPv6 traffic by December-2011. In addition, it has

come to light that small and medium service providers need guidance for transition. Therefore, a transition plan for all service providers is suggested in the document. **To start with all major Service providers (having at least 10,000 internet customers or STM-1 bandwidth) will target to handle IPv6 traffic and offer IPv6 services by December-2011.** This will be followed by smaller ISPs who need expertise and guidance for transition, which can be provided by the Network Implementation Working Group in the Task Force. All smaller ISPs shall make efforts to provide IPv6 services before exhaustion of IPv4 addresses.

-----X-----

REFERENCES

1. <http://www.coai.in> website of the Cellular Operators Association of India
2. <http://www.auspi.in> website of the Unified Telecom Service Providers of India
3. <http://www.trai.gov.in> website of the Telecom Regulatory Authority of India
4. <http://www.dot.gov.in> website of the Department of Telecommunications, India
5. <http://www.ipv6forum.org> website of the IPv6 Forum
6. Venkata Praveen Tanguturi, Fotios C. Harmantzis, *Broadband in India: Strategic Investment Opportunities*, Technology in Society 29 (2007) 431-440
7. Christopher Garbacza, Herbert G. Thompson Jr., *Demand for telecommunication services in developing countries*, Telecommunication Policy 31 (2007) 276-289
8. *3G, A New Era; Voice and Data*, October 2009
9. Annual Report 2008-2009, Department of Telecommunications
10. TRAI Report, *Indian Telecom Services Performance Indicators*, July-Sept 2009
11. Inputs from TEC IPv6 workshops in Delhi, Bangalore, Chennai & Mumbai
12. Moonv6: <http://www.moonv6.org>
13. MetroNet6: <http://www.cav6tf.org/html/metronet6.htm>
14. Occaid: <http://www.occaid.org>
15. U-Japan: http://www.suumo.go.jp/menu_02/ict/ujapan_en/index2.html
16. U-Korea: <http://www.ukoreaforum.or.kr>
17. CNGI: http://www.edu.cn/english_1369/index.shtml
18. AfriNIC: <http://www.afrinic.net>
19. AfNOG: <http://www.afnog.org>
20. European IPv6 Task Force: <http://www.eu.ipv6tf.org/>
21. IPv6 Forum: <http://www.ipv6forum.com>
22. 6bone: <http://www.6bone.net>
23. M6bone: <http://www.m6bone.net>
24. 6NET: <http://www.6net.org>
25. 6DISS: <http://www.6diss.org>
26. Euro6IX: <http://www.euro6ix.org>
27. GÉANT: <http://www.geant.net>

28. U-2010: <http://www.u2010.org>

29. Occasion: <http://www.ist-occasion.org>

ANNEXURE-A

TBSA/IPv6/TSTP-TEC-2008
Government of India
Ministry of Communications & IT
Department of Telecommunications
Telecommunication Engineering Centre

Dated 11th December 2009

Sub: Checklist for Migration from IPV4 to IPv6 in India

Sir,

The Government of India has recognized the importance of early transition from IPv4 to IPv6 in India and therefore given high priority for migration to meet the future growth in the Telecommunications and Internet space. TEC, which is the technical wing of the Department of Telecommunications, is coordinating the work of facilitating the smooth migration from IPV4 to IPV6 in India in consultation with different stakeholders. During the IPv6 workshops conducted by TEC, it has emerged that organizations need a checklist to list out the steps needed for migration. Accordingly, a general checklist is given below, which can be referred.

2. Preliminary Checklist for IPV6 compliance in organizations

- a) Deployment of IPV6 in the networks will be done in phases using technology solutions for interoperability of IPV4 and IPV6 networks. Currently there are 3 technology solutions devised by IETF (Internet Engineering Task Force), which will make this migration possible. These are –
 1. **Dual Stack (Dual IP)**
 2. **Tunneling Techniques**
 3. **Translation Techniques**
- b) The first thing that organizations would need to do is a proper auditing of the computers and networking equipments used in the organization to see if they are able to support the above methods.
- c) Similarly the operating systems and application software used in the organization should also be checked for IPV6 capabilities. The IPV6 support Capabilities of various Operating Systems are given below –

Vendor	Operating System	Reference
Apple	Mac OS 10.2 and later	http://developer.apple.com/macosx/
BSD	Free BSD 4.0 and later Open BSD 2.7 and Later Net BSD 1.5 and Later BSD/OS 4.2 and Later	http://www.kame.net
HP	HP-UX 11i and Later Tru64 UNIX V5.1 and Later Open VMS V5.1 and Later	https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1306AA http://h30097.www3.hp.com/unix/v51b.html http://h71000.www7.hp.com/doc/732final/6645/6645pro_index.html
IBM	AIX 4.3 and Later OS/390 V2R6 eNCS z/OS Rel 1.4 and Later	http://www-306.ibm.com/software/os/zseries/ipv6/
Linux	Rel 6.2 and later Mandrake 8.0 and Later SuSE 7.1 and later Debian 2.2 and later	http://www.bieringer.de/linux/IPV6/status/IPV6+Linux-status-distributions.html
Windows	Windows2000 - IPv6 technology preview on Windows 2000, but did not provide support. Window XP - Got a supported IPv6 stack but with a limited subset of supported applications such as Internet Explorer 6.0, Window Media Player 9.0 and 10.0, and Conference XP 3.2, but no IPv6 support for popular applications Window vista - IPV6 implementation is available. Parity between IPv4 and IPv6 at the application level.	Reference – http://www.microsoft.com/ipv6
Novell	Netware 6.1 and Later	
SUN	Solaris 8 and Later	http://www.sun.com/software/solaris
Symbian	Symbian 7.0 and Later	http://www.symbian.com

- d) Once the IPv6 compliant and non-compliant equipments and software are identified, a transition plan shall be made for procurement of IPV6 compliant hardware and software for replacing the non-compliant hardware and software over a period of time.
- e) The nodal officers will take up the creation of IPv6 transition teams. They will also prepare a transition plan specific to their organization in consultation with their service provider.
- f) Service providers giving the internet and leased line connections will be asked to provide IPV6 connectivity to the organization.
- g) Meanwhile all new equipment purchases should be ensured that they are IPV6 compliant and able to support IPV6 without upgrades.
- h) Set up a pilot IPV6 network in the organization, which will be used for training of staff and testing purpose also.
- i) Application migration can start by designing the organization website to support IPV6 so that customers can browse the website using both IPv4 and IPv6 protocol.

It is hoped that this will help in planning and implementing IPV6 in the organization in a smooth manner.

Yours sincerely



(B.K.Nath)
Dir(SA-III), TEC
Ph: 23329062

To

All Nodal Officers

ANNEXURE-B

Checklist for Assessment of Existing Network Infrastructure

This checklist is to identify IPv6 compliance for existing networking peripherals, software and services.

Technical Personnel Detail	
Name	
Tel	
Fax	
Email	

1. Devices

1.1 Network Device (Layer 2)

Identify Network Device (3Com Switch, Cisco Series Switches or any other switches etc.)					
Device ID	Name	Model	Firmware	Manufacturer	IPv6 Support

1.2 Network Device (Layer 3)

Identify Network Device (Cisco 7200 Router etc.)					
Device ID	Name	Model	Firmware	Manufacturer	IPv6 Support

1.3 Security

Identify Security Device (firewall, IDS, etc.)					
Device ID	Name	Model	Firmware	Manufacturer	IPv6 Support

1.4 Network Management (hardware base)

Identify Management Tool Device (Ciscoworks, etc.)					
Device ID	Name	Model	Firmware	Manufacturer	IPv6 Support

2. Operating Systems

2.1 Server

Identify Operating System for Server (Windows 2000, Linux etc.)			
Operating Systems	Purpose	Version	IPv6 Support

2.2 Client/Host

Identify Operating System for Hosts (Windows XP, Fedora etc.)			
Operating Systems	Purpose	Version	IPv6 Support

3. Network Service

3.1 Email

Identify Application for Services (pop3, smtp..etc)			
Application	Package	Version	IPv6 Support

3.2 Remote Shell

Identify Application for Services (telnet,ssh..etc)			
Application	Package	Version	IPv6 Support

3.3 File Sharing

Identify Application for Services (samba, tftp..etc)			
Application	Package	Version	IPv6 Support

3.3 Domain Name System

Identify Domain Name System Server application (bind, dbind..etc)			
Application	Package	Version	IPv6 Support

4. Network Application

4.1 Monitoring

Identify Network Configuration tools/applications (mrtg, nmap, tcpdump etc.)			
Application	Package	Version	IPv6 Support

4.2 Production

Identify office production tools (email client, Microsoft office etc.)			
Application	Package	Version	IPv6 Support

4.3 Web Server

Identify Web Servers (apache 1.3.37, Lighttpd 1.4.16, etc.)			
Application	Package	Version	IPv6 Support

4.4 DNS Server

Identify DNS Server (BIND 9.3.4, Windows Server 2003 DNS,...etc)			
Application	Package	Version	IPv6 Support

4.5 Email Server

Identify Email Server (Postfix & Dovecot, Sendmail & Cyrus IMAPD...etc)			
Application	Package	Version	IPv6 Support

4.6 Proxy Server

Identify Proxy Server (Squid Cache 2.6.STABLE12 + IPv6 Patch, Apache 2.0.59...etc)			
Application	Package	Version	IPv6 Support

4.7 Database Server

Identify Database Server (MySQL , Microsoft SQL 2000 / 2005...etc)			
Application	Package	Version	IPv6 Support

5. Sign Off

This is to certify that the Check List for Implement IPv6 has been completed successfully.

.....

Review & Confirm By:

Title:

Agency:

IPv6 Migration Strategies

Introduction to IPv6 Migration

1. The huge Internet size and the unlimited number of IPv4 users today make it inappropriate to migrate from IPv4-only to IPv6-only. As organizations are depending more on the Internet to perform their daily tasks, the downtime to replace the protocol will not be tolerated. Thus, the best alternative will be the co-existence of the both protocols at the same time and the migration should be implemented node by node based on the autoconfiguration procedures which makes it unnecessary to configure IPv6 hosts manually. This will be the best way for users to derive the IPv6 advantages while still being able to communicate with IPv4 devices.
2. There are a number of requirements that has been identified as the way IPv6 services should be introduced in a network such as:
 - a. The current existing IPv4 services should not be adversely disrupted as such situation might happen when router loading process of encapsulating IPv6 in IPv4 for tunnels;
 - b. IPv6 services should perform as well as the IPv4 services (For instance, at the IPv4 line rate and with similar network characteristics);
 - c. The services must be easily managed and monitored whereby tools should be available for both the protocols;
 - d. Network security should not be at stake because of the additional protocol itself or loophole of if any, the transition mechanism used; and
 - e. A plan for IPv6 address allocation should be created.

Requirements for the Transition to IPv6

The requirements that should be met when creating the transition part of the migration plan according to RFC1752 (The Recommendation for the IP Next Generation Protocol) are as below:

- (a) Incremental upgrade whereby upgrading for IPv4 devices to IPv6 with no dependencies on other devices.
- (b) Incremental deployment whereby new IPv6 devices can be installed with no prerequisites.
- (c) Easy addressing in which the upgrading of IPv4 devices to IPv6 allows the current addressing to continually be used.
- (d) Low start-up costs, as not much preparation work is necessary to upgrade the current IPv4 systems to IPv6 or deploying the new IPv6 systems.

Transition Techniques

The migration from IPv4 to IPv6 will be done one step at a time, initiating from a single host or subnet. Deployment of IPv6 in a large-scale network will require more than just one technique according to the various demands and requirements of the network. The three main transition techniques are:

a) Dual Stack

- (i) Dual Stack mechanism is one of the simplest methods of introducing IPv6 to a network and is also the best way for IPv4 and IPv6 to co-exist in the same time before the complete transformation to IPv6-only network in the future. With the dual-stack technique, a host or router has IPv4 and IPv6 protocol stacks in the operating system. IPv4 and IPv6 addresses are configured into each IPv4/IPv6 node whereby the node can send and receive datagram and communicate with nodes in the IPv4 combined with IPv6 network. Dual stack scenario does not require any real transition mechanism as it can integrate IPv6 by itself.
- (ii) The issue of deploying an IPv4/IPv6 dual stack network is the configuration of internal and external routing for IPv4 and IPv6 protocols. The interaction of the IPv4 and IPv6 protocols is

also a challenge as it is necessary to oversee the management of the interaction, whereby the dual-stack network mostly be interacting with IPv4 external networks in the beginning of the IPv6 deployment.

- (iii) Basically, a network or backbone becomes dual-stack if the routers and switches in the network routes both IPv4 and IPv6. The implementation of the dual-stack technique will require the upgrading of routers to dual-stack which supports both IPv4 and IPv6 addresses. In a dual-stack implementation, access to IPv6 Domain Name System (DNS) as well as adequate memory for both IPv4 and IPv6 is necessary. The challenges that might arise during dual-stack implementation are memory and CPU exhaustion as well as the need to introduce additional security requirement. Thus, steps should be taken to ensure that these issues and challenges do not arise; and a more smooth and cost-effective solution is obtained.

(b) Tunneling

- (i) Tunneling or encapsulation techniques used in the migration from IPv4 to IPv6 simply means that IPv6 is used on top of the current IPv4 infrastructure with no changes made to the routers or IPv4 routings. Tunnels encapsulate the IPv6 packets in IPv4 packets and are carried out to the network parts that are not IPv6 enabled. Tunneling technique is used only when the network is not able to offer native IPv6 functionality. The tunneling technique is used when the network is not at all or partly offering native IPv6 functionality. There are generally three steps involved in the tunneling process such as encapsulation, decapsulation and tunnel management. Two tunnel endpoints are required for the tunneling process. Most of the time the tunnel endpoints are IPv4/IPv6 dual-stack nodes which most of the time are the routers.

- (ii) Tunneling is considered a practical approach to the transition from current IPv4 networks adopting the IPv6 technology but as there are quite a number of existing tunneling mechanisms, it is a difficult task to choose the right tunneling mechanisms.
- (iii) There are varieties of methods for carrying IPv6 over existing IPv4 networks through either manually or automatically configured tunneling mechanism. The various kind of tunneling mechanisms includes configured tunnel; tunnel broker; automatic tunnels; 6to4; 6over4; ISATAP; Teredo; Tunnel Setup Protocol (TSP); DSTM; and Open VPN-based tunneling solution.

(c) Translation Methods

Translation methods are basically used when an IPv4-only device wants to communicate with an IPv6-only device, or vice-versa. Most importantly, IPv4-in-IPv6 is not used in this case. The various translation methods includes Stateless IP/ICMP Translation Algorithm (SIIT), Network Address Translation with Protocol Translation (NAT-PT) and Network Address Port Translation with Packet Translation (NAPT-PT); Bump-in-the-Stack (BIS); Bump-in-the-API (BIA); Transport Relay; SOCKS; Application Layer Gateway (ALG);

Node Types

1. RFC 2893, “Transition Mechanisms for IPv6 Hosts and Routers,” defines the following node types:
 - (a) **IPv4-only node** Implements only IPv4 and is assigned only IPv4 addresses. This node does not support IPv6. Most hosts—such as client computers, server computers, and network-capable devices such as printers—and routers installed today are IPv4-only nodes.
 - (b) **IPv6-only node** Implements only IPv6 and is assigned only IPv6 addresses. An IPv6-only node is only able to communicate with IPv6 nodes and IPv6-enabled applications. Although this type of node is not common today, it will become more prevalent as smaller devices such as cellular phones and handheld computing devices include only IPv6 stacks.
 - (c) **IPv6/IPv4 node** Implements both IPv4 and IPv6 and is assigned both IPv4 and IPv6 addresses. Computers running Windows Server 2008 or Windows Vista are by default IPv6/IPv4 nodes.
 - (d) **IPv4 node** Implements IPv4 and can send and receive IPv4 packets. An IPv4 node can be an IPv4-only node or an IPv6/IPv4 node.
 - (e) **IPv6 node** Implements IPv6 and can send and receive IPv6 packets. An IPv6 node can be an IPv6-only node or an IPv6/IPv4 node.

Comparison of transition techniques

1. Dual-Stack

- (a) Easy to use and flexible technique.
- (b) Host can communicate with IPv4 hosts via IPv4 or communicate with IPv6 hosts via IPv6.

- (c) IPv4 stack can be disabled when everything is fully IPv6.
- (d) The greatest flexibility is obtained in deploying dual-stack hosts and routers as it deals with IPv4-only applications, equipments and networks.
- (e) Dual-stack is a basis of the other transition techniques as tunnels need dual-stack endpoints and translators need dual-stack gateways.
- (f) The disadvantage of this technique is that when there are two separate protocol stacks running, an additional CPU power and memory is required on the host.
- (g) As all tables are kept twice with one per protocol stack, a DNS resolver who runs on the dual-stack host must be able of resolving both IPv4 and IPv6 address types.
- (h) Applications that run on the dual-stack host must be able to determine on whether the host is communicating with an IPv4 or IPv6 peer.
- (i) There is a necessity to have a routing protocol that is able to deal with IPv4 and IPv6 protocol (e.g. IS-IS which deals with both protocol); or routing protocols that deals with the both protocol separately (e.g. OSPFv2 for IPv4 network) and (OSPFv3 for IPv6 network).
- (j) Firewall must be able to protect both IPv4 network and the IPv6 network; as well as separate security concepts and firewall rules for each of the protocol.

2. Tunneling

- (a) This technique allows the migration of IPv6 to take place the way the user wants.
- (b) A specific order is not present for this technique as the upgrade of single hosts or single subnets can be done within a network and can connect to separate IPv6 clouds via tunnels.
- (c) ISP support for IPv6 to able to access remote IPv6 networks is not necessary as tunneling is possible via IPv4 infrastructure.
- (d) The upgrading of the backbone is not needed as if the backbone is IPv4, tunneling can be done to transport IPv6 packets over to the backbone.
- (e) With an MPLS infrastructure, it is better to use this technique to tunnel the

IPv6 packets if there is no necessity of upgrading the backbone routers to support IPv6 natively.

- (f) The setback of this technique is additional load is placed on the router.
- (g) The tunnel entry and exit points also need more time and CPU power to encapsulate and decapsulate packets.
- (h) Complex troubleshooting as it is likely to have hop count or MTU size issues and also fragmentation issues. Managing encapsulated traffic such as per-protocol accounting is also tougher because of the encapsulation.
- (i) Tunnels also rises security attack points.

3. Translation

- (a) Translation technique should only be used when other techniques are not suitable.
- (b) Translation should be a temporary solution till the other techniques can be used.
- (c) The setback of this technique is advanced IPv6 features such as end-to-end security is not supported.
- (d) The design topology has limitations as there are no replies from the same NAT router that was initially sent.
- (e) NAT routers are viewed as a single point of failure and it is not able to use the flexible routing mechanisms.
- (f) Applications with IP addresses in the packets payload will stumble.
- (g) The benefit of translation technique is IPv6 host's direct communication with IPv4 hosts and vice versa is allowed.

GLOSSARY

Sl. No.	Abbreviation	Meaning
1	2G	2 nd Generation
2	3G	3 rd Generation
3	6INIT	IPv6 Internet Initiative
4	6NET	3 year European Project to demonstrate that continued growth of the Internet can be met using new IPv6 Technology
5	6WINIT	IPv6 Wireless Internet Initiative
6	ACTO	Association of Competitive Telecom Operators
7	APNIC	Asia Pacific Network Information Centre
8	APT	Asia Pacific Telecommunity
9	ARPU	Average Revenue Per User
10	ASN	AS Number, Autonomous System Number
11	AUSPI	Association of Unified telecom Service Providers Association of India
12	BCG	Boston Consulting Group
13	BSNL	Bharat Sanchar Nigam Limited
14	BWA	Broadband Wireless Access
15	CATV	Cable TV
16	CCTLD, ccTLD	Country Code Top level Domain
17	CDMA	Code Division Multiple Access
18	CDOT	Centre for Development of Telematics
19	CETTM	Centre for Excellence in Telecom Technology and Management
20	CMAI	Component Manufacturers Association of India
21	CNGI	China Next Generation Internet
22	COAI	Cellular Operators Association of India
23	CTIA	Cellular Telephone Industries Association
24	DECT	Digital Enhanced Cordless Telecommunications
25	DEL's	Direct Exchange Lines

26	DHCP	Dynamic Host Configuration protocol
27	DIT	Department of Information Technology
28	DNS	Domain Name System
29	DSL	Digital subscriber Line
30	ERNET	Education and Research Network
31	ETSI	European Telecommunications Standards Institute
32	EUv6TF	European Union IPv6 task Force
33	FMC	Fixed to Mobile Convergence
34	FMCG	Fast Moving Consumer Goods
35	FTTH	Fiber To The Home
36	GDP	Gross Domestic Product
37	GIS	Geographic Information System
38	GOI	Government of India
39	GPRS	General Packet Radio Service
40	GSM	Global System for Mobile communications
41	HDVoD	High Definition Video on Demand
42	HHI	Hirschman Herfindahl Index
43	IANA	Internet assigned Numbers Authority
44	ICANN	Internet Corporation for Assigned Names and Numbers
45	ICMP	Internet Control Messaging Protocol
46	ICT	Information and Communication Technologies
47	IETF	Internet Engineering Task Force
48	IIT	Indian Institute of Technology
49	IP	Internet Protocol
50	IPTV	Internet Protocol Television
51	IPTV	Internet Protocol Television
52	IPv4	Internet Protocol version 4
53	IPv6	Internet Protocol version 6
54	ISP	Internet Service Provider
55	ISPAI	Internet Service Providers Association of India

56	ITU	International Telecommunication Union
57	LTE	Long Term Evolution
58	MIPv6	Mobile IPv6
59	MNP	Mobile Number Portability
60	MOU	Memorandum of Understanding
61	MPLS	Multiprotocol Label Switching
62	MTNL	Mahanagar Telephone Nigam Limited
63	MTU	Maximum Transmission Unit
64	MVNO	Mobile Virtual Network Operators
65	NAT	Network Address Translation
66	NAV6TF	North American IPv6 Task Force
67	NGN	Next Generation Networks
68	NIXI	National Internet Exchange of India
69	NTP	National Telecom Policy
70	PDA	Personal Digital Assistant
71	PEST	Political, Economic, Social and Technological
72	PPP	Public Private Partnership
73	PSU	Public Sector Undertaking
74	QoS	Quality of Service
75	RFC	Request for Comments
76	RFID	Radio Frequency Identification
77	RIR	Reginal Internet Registry
78	RTP	Real Time Transport Protocol
79	SCSI	Small Computers Systems Interface
80	SIP	Session Initiation Protocol
81	SSL	Secure Socket Layer
82	SWOT	Strengths, Weaknesses, Opportunities and Threats
83	TCP	Transmission control protocol
84	TDSAT	Telecom Disputes Settlement and Appellate Tribunal
85	TEMA	Telecom Equipment Manufacturers' Association

86	TRAI	Telecom Regulatory Authority of India
87	TTL	Time to Live
88	U-2010	Ubiquitous IP Centric Government and Enterprise Next Generation Network, Vision 2010 ¹
89	UDP	User Datagram protocol
90	UNH-IOL	University of New Hampshire Interoperability Laboratory
91	USO	Universal Service Obligation
92	V6PC	IPv6 Promotion Council
93	VAS	Value Added Service
94	VPN	Virtual Private Network
95	WIDE	Widely Integrated Distributed Environment
96	WiMAX	Worldwide Interoperability for Microwave Access
97	XML	Extensible Markup Language

¹ Project of the European Union

REGIONAL INTERNET REGISTRIES



TELECOMMUNICATION ENGINEERING CENTRE

Department of Telecommunications

Ministry of Communications & Information Technology

Government of India

Gate No. 5, Khurshid Lal Bhawan, Janpath, New Delhi-110001

Website : <http://www.tec.gov.in>